german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by:
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

**Fight Money Laundering with Personal Data Protection**
**New EU Directives**

# ASSESSMENT

of the national legal and institutional approximation with the 4th and 5th EU AML directives with the focus on data protection in the AML/CFT regulations in Albania, Kosovo, North Macedonia and Montenegro

TRANSPARENCY INTERNATIONAL
MACEDONIA

**For TI Macedonia**

Slagjana Taseva Ph.D, Team Leader and Author of the Project

Metodi Zajkov, Secretary General

This publication was produced with the financial supported by GIZ as commissioned by the Federal Ministry for Economic cooperation and development of Germany and the Ministry of Foreign Affairs of Norway. Its contents are the sole responsibility of Transparency International – Macedonia and do not necessarily reflect the views of the donors.

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

[343.9.024:336.7]:341.24(4-672ЕУ)
[343.9.024:336.7]:342.5.072.3(4-672ЕУ)
342.738(497.7:4)

FIGHT money laundering with personal data protection new EU directives [Електронски извор]: assessment of the national legal and institutional approximation with the 4th and 5th EU AML directives with the focus on data protection in the AML/CFT regulations in Albania, Kosovo, North Macedonia and Montenegro / Slagjana Taseva ... [и др.]. - Skopje : Transparency International - Macedonia, 2022. - 202 стр. :
илустр. ; 30 см

Достапно и на:
https://transparency.mk/wp-content/uploads/2022/02/fight_money_laundering_with-persoal_data_protection-1.pdf.
- Текст во PDF формат, содржи 202 стр., илустр. - Наслов преземен од екранот. - Опис на изворот на ден 04.02.2022. - Фусноти кон текстот. - Други автори: Elena Andreevska, Biljana Papović, Ivan Vukcević, Besa Tauzi, Zamira Nurce, Ehat Miftaraj, Yll Zekaj, Elisabeth Florkowski, Graham Sutton

ISBN 978-608-66251-7-7

1. Taseva, Slagjana [автор] 2. Andreevska, Elena [автор] 3. Papović, Biljana [автор] 4. Vukcević, Ivan [автор] 5. Tauzi, Besa [автор] 6.
Nurce, Zamira [автор] 7. Miftaraj, Ehat [автор] 8. Zekaj, Yll [автор] 9.
Florkowski, Elisabeth [автор] 10. Sutton, Graham [автор]
а) Перење пари -- Меѓународно-правна регулатива -- Европска Унија б) Перење пари -- Спречување -- Европска Унија в) Заштита на лични податоци
-- Македонија -- Европа

COBISS.MK-ID 56269829

german cooperation
DEUTSCHE ZUSAMMENARBEIT

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

# Assessment

of the national legal and institutional approximation with the 4th and 5th EU AML directives with the focus on data protection in the AML/CFT regulations in Albania, Kosovo, North Macedonia and Montenegro

TRANSPARENCY INTERNATIONAL MACEDONIA

**January 2022**

**Skopje, Republic of North Macedonia**

## ACKNOWLEDGEMENTS

The objective of the assessment is: "To provide countries with timely assessment of the national legal and institutional approximation with the 4th and 5th EU AML directives with the focus on data protection in the AML/CTF regulations." This assessment of how the anti-money laundering regulations respect the data protection in the four countries: Albania, Kosovo, Montenegro and North Macedonia is part of the Transparency International Macedonia's continuous cooperation with GIZ that empowers civil-society actors in the countries from the region to identify, analyze and map new trends in the AML/TF regime and the impact of these on illicit flows, governance, development, inter-ethnic relations, security and the rule of law, and supports them in their monitoring of national dynamics and wider regional and international organized-crime trends.

The report is based on data, information and analyses collected by civil-society actors. In particular, it draws on desk research, interviews and focus groups from eight experts in Albania, Kosovo Montenegro and North Macedonia. We thank them for their valuable contributions and frank and constructive engagement throughout the process. Special thanks to Slagjana Taseva, Elena Andreevska, Biljana Papovic, Ivan Vukcevic, Ehat Miftaraj, Yll Zekaj, Besa Tauzi, Zamira Nurce, Stefanija Mladenovska for their hard work in designing the methodology, coordination, data collection, analysis and synthetizing of the collected data, to be used by the two international experts Ms. Elisabeth /Lisa Florkowski and Mr. Graham Sutton. It has been a great challenge to provide this type of assessment that has non-precedence that could be used as a guide. Therefore, the regional partners accepted the challenge without being previously involved specifically in AML/TF related work. This is why the reader will find reports different in structure but with solid content to serve for the report presented by the international experts. Lisa and Graham made an exquisite effort that resulted with guiding recommendations that will serve wider than just in the region.

This publication was produced with the financial supported by GIZ as commissioned by the Federal Ministry for Economic cooperation and development of Germany and the Ministry of Foreign Affairs of Norway. Its contents are the sole responsibility of Transparency International – Macedonia and do not necessarily reflect the views of the donors.

## ABOUT THE AUTHORS:

**Ms. Elisabeth/Lisa Florkowski** is **Independent Consultant for AML/CFT and** Registered Advisor with Austrian Chamber of Commerce. She has experience in compliance side and knowledge of all aspects of the preventive side of AML/CFT regimes that brough this work close to international standards and practices and enable the whole team to identify the real aspects of concerns arising from the two dimensions covered by the two Directives that were subject of analysis.

**Mr. Graham Sutton** is a freelance consultant in data protection and access to official information (together referred to here as information rights) with extensive experience in Europe and beyond of providing advice on the development of information rights law and practice, and of speaking at training events on information rights. Being a UK civil servant Mr. Sutton advised UK Government on all aspects of data protection policy including his membership of UK team's that negotiated EU Data Protection Directive (95/46/EC) and led team that prepared legislation transposing Directive into UK law (Data Protection Act 1998) and many other relevant activities.

# ACKNOWLEDGEMENT TO THE AUTHORS OF THE COUNTRY ASSESSMENT REPORTS

**Macedonian Team:**

**Slagjana Taseva, Ph.D**
**Elena Andreevska, Proffesor**

**Montenegro team:**

**Biljana Papović**
**Ivan Vukcević**

**Albanian team:**

**Besa Tauzi**
**Zamira Nurce**

**Kosovo team:**

**Ehat Miftaraj**
**Yll Zekaj**

I. Introduction ..... 5
II. Interface of DP and AML/CFT ..... 6
III. Aim of the Fight against Money Laundering and Terrorism Financing – European Union AML Directive Aim ..... 7
IV. European Union ..... 8
V. Data Protection within the EU ..... 9
VI. Provisions of AML Directive Requiring the Processing of Personal Data ..... 10
Table of AMLD Provisions requiring Data Processing ..... 11
VII. Practices & Problems– Current Status in EU jurisdictions ..... 13
VIII. Analysis of Status of the four Countries ..... 14
IX. The views of the European Data Protection Supervisor (EDPS) ..... 14
X. GENERAL POINTS ON THE FOUR COUNTRIES ..... 16
XI. Transposition of the EU legal instruments ..... 16
XII. Practice ..... 16
XIII. International co-operation ..... 17
XIV. Analysis of the 6 Categories of AMLD Subjects in Table above ..... 18
XV. Private Sector Bodies – Obliged Entities in AMLD ..... 18
XVI. Supervisory bodies ..... 19
XVII. Supervisors in their core function ..... 19
XVIII. Supervisors guiding their supervised entities ..... 20
XIX. Note on FIU as Supervisor ..... 20
XIX. Holders of Registers ..... 20
XX. Financial Intelligence Units (FIUs) ..... 21
XXI. Law enforcement bodies, Prosecutors and Courts ..... 21
XXII. Recommendations and Conclusions ..... 22
XXIII. Recommendations ..... 23
XXIV. Conclusions ..... 25
XXV. Annexes ..... 27
ANNEX 1. COUNTRY REPORT REPUBLIC OF NORTH MACEDONIA ..... 28
ANNEX 2. COUNTRY REPORT KOSOVO ..... 86
ANNEX 3. COUNTRY REPORT MONTENEGRO ..... 111
ANNEX 4. COUNTRY REPORT ALBANIA ..... 162

# Relationship between data protection and aml/cft in a practical review of the overall approach of the four countries

## I. INTRODUCTION

1. This paper was prepared as part of the project set up with the aim of making the assessment set out in the title above. As well as their close geographical location, the four countries have in common the ambition of joining the European Union. Realising this ambition will require them to achieve the standards set by the EU's acquis communautaire including in the fields of Anti Money Laundering/Countering Terrorism Financing (AML/CFT) and data protection (DP). Experts mandated by TI studied the relationship between data protection and AML/CFT in a practical review of the overall approach of the 4 countries in the title from April 9th to May 31st, 2021 in order to provide an overview of relevant topics and strategic recommendations at regional level.

2. The aim of this broad overview is to allow practitioners who are familiar with either Data Protection or Anti Money Laundering/Countering Terrorism Financing in their professional capacity to rapidly see the intersections between the two topics, and therefore to support them in framing an adequate strategic response concerning their specific needs.

3. The analysis in this paper builds upon local experts' review of the relevant laws, and on the findings set out in their reports. It should therefore be read in conjunction with the separate reports for each of the 4 countries. It does not cover the detailed review of current Laws and Regulations that was done in these reports, and it does not stand separate from their assessments. Its main purpose is not to identify any gaps that there might be in any individual country's arrangements. Rather, it offers an overview aimed at policy and strategy concerns both at national level and in the various institutions involved in AML/CFT.

4. It is the international experts' wish to highlight an example of best practice from each country right at the beginning of this report to applaud efforts made and encourage other countries, not only in the region but also in the EU or globally, to read this report with such models of good work in mind:

    a. In Albania the DPA has conducted an audit of the FIU, the holder of the Beneficial Owner Register and the holder of the Register of Bank Accounts and reported to Parliament about the outcomes so that any deficiencies may be addressed. Conducting such audits and ensuring parliamentary oversight is a very good practice that should be considered by other countries as well, not only in the region.

    b. The report from North Macedonia provides an excellent in-depth legal description and analysis which constitutes a good tool for developing regulations and rules based on the Laws and legal considerations in place. Detailed and well-crafted explanations of the current legal system, in a very approachable format for both types of legal experts, is a foundation that helps any further efforts.

    c. The report from Kosovo suggests that there is a very vibrant inter-agency communication, and a willingness of the AML/CFT prosecutors and associated law enforcement to debate

and engage on data protection – the open dialogue in this topic is a good example of an open search for the specific issues and their solution which can only be of profit. Though such a practice is probably most suited to small countries and jurisdictions, it is very valuable, and an informal foundation is often the building ground for new solutions that understand the specifics of each partner in the complex landscape of DP and of AML/CFT combined.

d. In Montenegro all the relevant bodies, including the Ministry of the Interior, the Police Administration, the FIU, the Ministry of Finance, the Supreme Court, the Supreme State Prosecutor's Office, the Judicial Council and the Central Bank have signed an agreement in the field of crime prevention. Formal agreements between responsible authorities are also a good practice, even where administrative cooperation is allowed and there is no formal need to create them – they strengthen awareness and provide details about the topics, specific process of cooperation and the designated channels, which is a great help to users in practice.

5. Documents and discussion papers, as well as an abbreviation list, used in this report are annexed.

## II. INTERFACE OF DP AND AML/CFT

EU legal instruments cover both topics thereby ensuring that there is a rule set at the highest level that must be taken into account equally. DP is covered by two EU instruments: a Regulation, the General Data Protection Regulation (GDPR) which applies to most of the activities carried out for anti-money laundering purposes; and a Directive, the Law Enforcement Directive (LED), which applies to certain law enforcement authorities when they carry out law enforcement activities. As a Regulation, the GDPR allows less flexibility at national level than the AMLD. However, the degree of detail expected in the AMLD, and also in the global standard covering this topic permits a very high degree of harmonization in the approach taken.

The AMLD requires the collection and analysis of large volumes of personal data, with the aim of preventing the financial services industry from being exploited as a means of laundering money and committing financial crimes. On the other hand, DP legislation, which has its origins in human rights and is there to protect individuals' information privacy, places restrictions on how, when and why personal data can be collected and used, among other things. Getting the relationship between the two instruments right is, therefore, of great importance. It also needs to be stressed that, the DP legislation applies to all organisations whether or not they are involved in AML/CFT activities. The AMLD adds only a small number of requirements to the general DP rules.

In this paper we set out the main aim and central topics of the AMLD and the GDPR. Because of its limited relevance to the work in this field, and also because the main rules that it sets are broadly similar to those in the GDPR, we do not look separately at the LED. We also set out a summary of the most relevant elements of the Opinion of the European Data Protection Supervisor (EDPS) on the European Commission's 2020 action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (the Commission's Action Plan) to show the topics raised and the work ahead at EU level. Then, a brief description of the data uses and data users in AML/CFT leads us into an assessment of the situation in the 4 countries in question.

# III. AIM OF THE FIGHT AGAINST MONEY LAUNDERING AND TERRORISM FINANCING – EUROPEAN UNION AML DIRECTIVE AIM

The Financial Action Task Force (FATF) as the global body leading this topic has graphically described the aim and methods of AML/CFT in the way set out in the table below. It focuses not so much on specific steps to take, but on effective results achieved. FATF's global standard covers 11 so called immediate outcomes, meaning that these 11 goals should be achieved in a demonstrable effective way by all countries and jurisdictions who wish to be part of the global cooperation, and particularly the global financial system. These goals are supported by a detailed standard of 40 Recommendations and additional technical documents, which are all helping in explain how to achieve the aims in the 11 immediate outcomes.

Non-fulfilment of the standard leads to gradually more stringent exclusion from many forms of international cooperation, focused on the global financial system, in an escalating approach of evaluation, request for improvement with deadlines, and further negative steps such as listing on grey or black lists with connected penalties. Practically all countries and jurisdictions globally are in an active relationship with FATF or its regional bodies and are evaluated constantly, with publication of the names of countries who do not achieve sufficient results in the fight against illicit financial flows and financial crime, on the website of FATF (*www.fatf-gafi.org*) three times a year. Such countries are seen as posing a threat to the integrity of the global financial system. Rapid remediation of any such threats is a necessity for any country who wishes to have a healthy economy and good international investment, trade and financial relations.

For the countries in the region, Moneyval is the direct partner, who is the FATF style regional body in charge of this geographical region. All action by Moneyval is strictly aligned with the FATF standard, and its methodology in all particulars.

These immediate outcomes are described in the FATF's own graphic below, giving an overview of all the topics that are part of the AML/CFT requirements to be achieved:

www.fatf-gafi.org, *2021*

All of the FATF measures in the overview above described under 2 to 11 touch upon data processing to a significant extent and are therefore covered in the report. Item 1 would usually be dealing with aggregate data and is not covered by the considerations below.

# IV. EUROPEAN UNION

## A. AML Directive's aim

The European Union closely follows the global standard and its ongoing developments both as a Member of FATF and in its own areas of responsibility, strongly supporting national legislation in all Member States who are committed to this fight and cover the topics where there is no EU mandate.

The AML Directive – currently the 4th AML Directive, Directive (EU) 2015/849, amended by the 5th AML Directive, Directive (EU) 2018/843, is in force and the 6th is in discussion – aims to prevent the use of the Union's financial system for the purposes of money laundering and terrorist financing.

The EU states that *it is essential that gatekeepers (banks and other obliged entities) apply measures to prevent money laundering and terrorist financing. Traceability of financial information has an important deterrent effect. The European Union adopted the first anti-money laundering Directive in 1990 in order to prevent the misuse of the financial system for the purpose of money laundering. It provides that obliged entities shall apply customer due diligence requirements when entering into a business relationship (i.e. identify and verify the identity of clients, monitor transactions and report suspicious transactions). This legislation has been constantly revised in order to mitigate risks relating to money laundering and terrorist financing (https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en ).*

## V. DATA PROTECTION WITHIN THE EU

Article 16 of the Treaty on the Functioning of the EU says that "Everyone has the right to the protection of personal data concerning them". This right is elaborated upon in Article 8 of the EU Charter of Rights, which sets out three basic requirements.

- Personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.
- Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
- Compliance with the rules must be subject to control by an independent authority.

All of these provisions of Article 8 are in their turn considerably further developed, and complemented by other provisions, in the three legal instruments which regulate the processing of personal data within the EU. For the purposes of this paper the most relevant is Regulation (EU) 2016/679 (the GDPR). In view of this, in this paper data protection references will be to the GDPR unless otherwise specified.

### The main elements of Data Protection

1. "Personal data" means any information about an identified or identifiable individual (the data subject). "Processing" includes anything at all that is done with personal data, from their collection through to their destruction, including merely holding them.

2. The main rules for processing personal data are that

   - processing must be consistent with the data protection principles set out in Article 5 of the GDPR. These cover requirements for fairness and lawfulness, purpose limitation, data adequacy, data accuracy, time limits for data storage, data security.
   - processing must be based on at least one of the legal grounds set out in Article 6 of the GDPR.
   - there are tighter grounds for the processing of special categories of data. (These are commonly referred to as "sensitive data" and cover matters such as an individual's political opinions, religious beliefs, health or sex life.)

- data subjects must be provided in advance by those doing the processing ("data controllers") with detailed information about the processing.
- data subjects have specified rights in relation to the processing of their data, including in particular the right to obtain access to the data on request.
- breaches of security must be noted to the data protection supervisory and, in some cases, to the data subjects.
- in some cases data controllers must appoint in-house data protection officers (DPOs) to ensure good practice within the organization.
- transfers of personal data to third countries are subject to special requirements;
- there must be an independent public body responsible for overseeing national implementation of the rules, and with powers of investigation and enforcement.

### Specific data protection provisions in the AML Directive

There are few specific data protection provisions in the AMLD. To the extent that Directive requires the processing of personal data, this means that the full regime of EU Data Protection law applies. This is confirmed by Article 41.1 of the AMLD which says that the processing of personal data under the AMLD is subject to Directive 95/46/EC (the Data Protection Directive which was the immediate forerunner of the GDPR) as transposed into national law. (It is not clear why Article 41.1 refers to the Data Protection Directive rather than to the GDPR, but there is no doubt about the intention.)

- Article 40 of the AMLD sets time periods for the retention of specified documents and information. As already noted, time limits for the storage of personal data are among the data protection principles. The AMLD sets more precise limits.
- Article 41.2 of the AMLD specifies the purposes for which obliged entities may process personal data.
- Article 41.3 of the AMLD specifies the time when an obliged entity must provide new clients with the information required to be provided to data subjects under Article 13 of the GDPR; and adds to the list of information mentioned in Article 13 of the GDPR a requirement to provide information about the legal obligations of the obliged entity under the AMLD.
- Article 41.4 of the AMLD deals with the steps which Member States must take in limiting data subjects' right of access to their personal data where the prohibition on disclosure set out in Article 39.1 of the AMLD applies.

## VI. PROVISIONS OF AML DIRECTIVE REQUIRING THE PROCESSING OF PERSONAL DATA

The Table below attempts to identify those articles of the AML Directive which require the processing of personal data by the following groups:

1. Private sector bodies
2. Financial Information Units (FIUs)
3. Holders of Registers

4. National financial sector supervisory bodies i.e. Central Banks or other dedicated financial market supervisors
5. Law enforcement bodies
6. Courts

The following further abbreviations are used in the Table:
OE – Obliged Entity
RA – Risk Assessment
EC – European Commission
DD – Due Diligence
CA – Competent Authority
PD – Personal Data
DP – Data Protection
DS – Data Subject

## Table of AMLD Provisions requiring Data Processing

| ARTICLE | EFFECT | GROUPS | **COMMENTS** |
|---|---|---|---|
| 7 | Requires Governments to do RAs taking account of data protection | | RAs will normally use aggregated data. |
| 8 | Requires OEs to do RAs | 1 | As above. Possibility of including specific clients' data in the RA. |
| 10 to 14 | DD by OEs | 1 | |
| 15 to 17 | Simplified DD by OEs | 1 | |
| 18 to 24 | Enhanced DD by OEs | 1 | |
| 25 to 29 | Delegation of DD by OEs to third parties | 1 | Where PD are involved, third parties will be data processors |
| 30.1 | Corporate bodies must hold and provide to OEs carrying out DD information about their beneficial ownership | 1 | |
| 30.2 | CAs and FIUs must have access to the information in A30.1 | 1, 2, 4 | |
| 30.3 and 30.4 | Information in A30.1 to be held in a central register | 1, 3 | Registers can be public. This has DP implications. |
| 30.5 | Amplifies 30.2 to 30.4 | 1,2,4 | |
| 30.6 | Requires access to central register by CAs and FIUs without alerting the entity concerned | 2,3,4 | Failure to inform must be justified under DP law |
| 30.10 | Interconnection of registers | 3 | Connection with registers in other countries requires data export rules to be met |
| 31 | Requires trustees to hold information about beneficial ownership of the trusts | 1,2,3,4 | Detailed provisions are similar but not identical to those applying to corporate bodies in Article 30. Similar DP considerations apply. |

| | | | |
|---|---|---|---|
| 32 | Establishment and functions of FIUs | 2 | |
| 32.4 | Collection of information by FIUs | 2,3,4 | |
| 32.5 | FIUs not obliged to provide requested information | 2,3,4 | If DS makes request, possible conflict with DP rules on subject access |
| 32a | Requirement for "centralised automated mechanisms". | 2,3,4 | |
| 32b | Information about real estate owners | 2,3,4 | |
| 33 | Reports by OEs to FIUs | 1,2 | |
| 34.1 | Certain OEs able to send reports to professional self-regulatory bodies instead of to FIUs | 1,2 | Position of self-regulatory bodies under DP law needs clarification. |
| 35 | Deferral of reports by OEs to FIUs | 1,2 | |
| 36 | CAs checking OEs to inform FIUs | 1,2,4 | |
| 37 | Disclosures in good faith by OEs | 1 | Overrides restrictions on disclosure in DP law. Point of difficulty needing clarification |
| 38 | Whistle-blowing | All | Concerns PD of both target of whistle-blowing and whistleblower |
| 39 | Disclosures by OEs | 1,4,5 | Affects data protection rules, including those on data exports |
| 40 | Record retention by OEs | 1 | Need for consistency with DP law |
| 41 | DP rules specific to AMLD | All | Need for consistency between specific rules and those in DP law |
| 42 | Requests to OEs from FIUs about specified persons | 1,2 | |
| 43 | Processing of PD under AMLD is a matter of public interest | All | Important for the legal base for processing of PD under DP law. Does **NOT** exempt processing from DP law. |
| 45 | Intra-group sharing of information by OEs | 1,4 | The rules on sharing information across national borders need to be consistent with those on data exports in DP law |
| 46 | OEs to keep employees informed | 1 | There is a reference to training which will be important for DP purposes |
| 47 and 48 | Functions of competent authorities | 1,4 | |
| 50a | Exchange of information among CAs in different countries | 4 | Arrangements need to be consistent with those on data exports in DP law |
| 53 | Sharing information among FIUs | 2 | As above |

| | | | |
|---|---|---|---|
| 55 | Use of shared information | 2,4 | Rules need to be consistent with those in DP law |
| 56 | Protecting shared information by technological means | 2 | Relates to DP by default and by design in DP law |
| 57a | CAs for credit and financial institutions including professional secrecy | 4,6 | The derogations from the requirement for secrecy need to be consistent with DP law |
| 57b | More on CAs for credit and financial institutions including international exchanges | 4,6 | Arrangements for international exchanges need to be consistent with rules on data exports in DP law |
| 58 to 62 | Sanctions | All | Sanctions, including publication of information identifying individuals involved, need to be consistent with DP law |

The AML concerned bodies are listed and numbered above in order of appearance in the AML Directive.

## VII. PRACTICES & PROBLEMS– CURRENT STATUS IN EU JURISDICTIONS

In EU jurisdictions, for all of the concerned AMLD practitioners above, work on ensuring the alignment of both sets of requirements is also challenging, and high level publications such as the EDPS opinion highlight that constant evaluation, care and questioning of emerging solutions in fighting illicit money flows are needed.

The intensity of personal data processing both in prevention of AML/CFT and in its detection and prosecution, asset recovery and the judicial processes involved is very high, so that questions of necessity and proportionality arise constantly. A single best practice actor, or sector, has not emerged yet to allow to refer to an existing best practice.

This is due to the fact that AML/CFT is risk based, and therefore by its very nature the intensity, depth and width of controls and data processing is not defined in detail ex ante. This leads to a case by case view of the amount and density of data to be collected and shared, and may result in conflict between different authorities on the actions that are still covered by the AML rules or already infringe data protection rules.

The main challenge appears to lie in areas where data are processed preventively without a specific criminal activity already having been identified. There, the understandable need to effectively recognize patterns of behaviour and thereby effectively interfere in illicit money flows leads to the collection, updating, monitoring and analysis of data on a very large scale.

Then, these data are reported to FIUs. They constitute information which is often not yet specifically suspicious, i.e. not linked yet to a criminal activity or person. It may really be suspicious activity, because the obliged entity sees behaviour that indicates a crime. On the other hand, it may be reporting based on the AMLD obligation for entities is to report also what is “large, complex and unusual” or “without clear economic purpose” or “where clients actual identity and source of funds/ wealth cannot be ascertained” according to the entity observing and reporting the business or transaction.

Reporting to the FIU also where there is no specific suspicion of a crime is necessary to allow for precious information to be analysed and shared by FIUs but both the amount of reporting and its

handling of data is one of the challenges everywhere, whether in the EU or in the four countries in the region, when it comes to the careful balance of effectively fighting illicit financial flows under the standard set out by FATF and AMLD, and data protection.

Looking forward, for the EU, the European Commission's 2020 Action Plan gives a view of the AML/CFT future that builds on six pillars:

- Effective implementation of existing rules
- A single EU rulebook
- EU-level supervision
- A support and cooperation mechanism for financial intelligence units
- Better use of information to enforce criminal law
- A stronger EU in the world

Based on this Action Plan, the Commission delivered a number of proposals to the EU Parliament in March 2021. These contain (i) a proposal to transfer parts of the existing Anti-money-laundering Directive to a regulation, thereby making it directly applicable in the Member States, (ii) EU level supervision with an EU-wide anti-money-laundering supervisory system, and (iii) a coordination and support mechanism for Member States' Financial Intelligence Units. This will affect all countries who wish to conform with EU standards, as all four countries do, once it becomes concrete and operational.

## VIII. ANALYSIS OF STATUS OF THE FOUR COUNTRIES

## IX. THE VIEWS OF THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

The EDPS is the data protection supervisory authority for the institutions, agencies and bodies of the EU. On 23 July 2020 he issued an Opinion on the European Commission's Action Plan which was published on 7 May 2020. The EDPS's Opinion was directed primarily at the European Commission but some of the points identified in the Press Release impinge directly on countries' AML/CFT activities.

> **(1) There is a need for a balance between the necessary measures to take for the general interest and the goals of the AML/CFT and the respect of the fundamental rights of privacy and personal data protection.**

Striking such a balance is, of course, a fundamental requirement. The best measure of how well the four countries have done is, perhaps, found in the extent to which they have properly implemented the relevant EU legislation. This is dealt with below.

> **(2) There is a need for a clear legal basis for the processing of personal data.**

The need for a legal basis for the processing of personal data has always been one of the essential requirements of data protection regimes. Since the four countries all claim to have data protection law in place, even though it may in some countries still be based on the EU 1995 Data Protection Directive rather than the GDPR, it may reasonably be assumed that they all satisfy this test.

> **(3) There is a need for specific rules for the access to and sharing of information, especially when personal data being processed are particularly sensitive.**

Since disclosing and sharing personal data are forms of processing, the data protection principles

regulate these activities in a general way. **The four countries' reports suggest that the extent to which there are specific rules regulating access and sharing is uneven**.

- One of the four countries has some specific rules on third party access to personal data for AML/CFT purposes but its report suggests that there is a "double standard" since data protection rules also had to be respected.
- Another country's report mentions the need to control third party access in the context of security requirements.
- Another report describes the, well developed but still incomplete, arrangements for third party access in some detail.
- The final report describes the position on third party access from the perspective of different interviewees. It appears that where there is such access it is based on Memoranda of Understanding between the parties rather than on the law.

**(4) There is a need for appropriate safeguards to guarantee compliance with the principles of data minimisation, purpose limitation and data protection-by-design.**

The principles of data minimisation and purpose limitation are also among the basic data protection principles which will have been established in the four countries' national data protection laws. As noted above, Article 41.2 of the AMLD sets the purposes for which obliged entities may process personal data. These purposes are somewhat more restrictive than those which apply to the generality of processing. When all the four countries have completed transposing the AMLD these more restrictive provisions, will no doubt be included. The best way of ensuring that there are appropriate safeguards in the three areas mentioned by the EDPS is for each of the four countries to have a functioning data protection supervisory authority (DPA) equipped with adequate powers to inform and advise obliged entities and other data controllers about the required standards and, where necessary, to take enforcement action.

**(5) There is a need for appropriate safeguards for the right of individuals to be informed when their data are collected and of the purpose(s) for which the data will be processed.**

In each of the countries, national data protection laws require this, and more, information to be provided to individuals. The national DPA has a central role to play here, too.

**(6) The EDPS supports the idea of Public Private Partnerships involving all the relevant actors to debate policy and other matters relating to AML/CFT provided that the exchanges have a sound legal basis and comply with data protection requirements.**

EU country experience shows that such PPPs, in particular where they focus on an open dialogue and thereby offer well targeted outreach and feedback as well as typologies and training to both sides, are very well received – the four countries are engaging in such dialogue and are encouraged to continue building such PPPs providing the data protection compliance required.

**(7) The EDPS is concerned that PPPs for the sharing of operational information on intelligence suspects by law enforcement authorities to obliged entities, may result in an unacceptable high risk for the individuals' rights to privacy and data protection.**

Exchanging intelligence information can be very useful in the fight against financial crime – EU countries experience that this needs to be handled with extreme care. **Clear written processes for setting up such an exchange, and for determining the participants, are key. The four countries would do well to ensure setting up a clear process ex ante between all stakeholders for such an exchange allowing cooperation on fighting financial crime within the data protection rules.**

## X. GENERAL POINTS ON THE FOUR COUNTRIES

Before looking at the position in the four countries according to the groups identified above, it may be helpful to make some general points and provide a flavour from the reports and interviews.

## XI. TRANSPOSITION OF THE EU LEGAL INSTRUMENTS

It is not altogether clear whether the four countries have fully transposed the AMLD and DP legislation yet. All the reports suggest that the four countries have good DP law in place, but it is not clear whether that law predates the GDPR and is, rather, a transposition of the GDPR's predecessor, the 1995 EU DP Directive. Moreover, the reports do not generally specify whether the limited, but nonetheless important, special data protection provisions set out in the AMLD have been incorporated into their national data protection regimes. **Probably, the best conclusion that can be drawn on the basis of the evidence provided in the reports is that implementation of the EU legislation across the four countries is patchy.**

Even in those countries where the reports suggest that transposition is largely complete, there is recognition that more work remains to be done. Effective transposition means more than simply writing the EU instruments into national law. National implementation of the EU instruments may well affect existing national primary and secondary legislation in addition to the main AML and data protection legislation. **The establishment of an effective AML regime which meets the requirements of data protection may also require adjustments to be made elsewhere in the national legislative framework.** Making sure that this is done, would help deal with the problem of legal uncertainty which was mentioned in some of the reports. It would, however, be unlikely to resolve that problem entirely since in difficult cases the exact relationship between the different laws will still depend upon the interpretation made by the courts.

## XII. PRACTICE

An effective regime requires more than having a sound legislative framework. Legislation needs to be complemented by good practice. This was widely recognised in the reports. As already mentioned, it is not the purpose of this paper to identify individual problems in particular countries, but one is of such significance that it cannot be ignored. **National DPAs play a pivotal role in ensuring not only compliance with national data protection law but also the development and promulgation of good practice.** In Kosovo, despite having had in place since 2019 a data protection law which makes provision for the appointment of a DPA, no such appointment has yet been made. This is a significant weakness in the arrangements in Kosovo which needs to be addressed as a matter of urgency.

Some of the reports mention a lack of awareness on the part of the stakeholders and their staff, or among the public, or both of these**. There are some indications that the stakeholders and/or their staff do not know how to handle the relationship between AML and data protection.** An example of this, which was mentioned in one report is the lack of a clear understanding of what is meant by "purpose", where it was suggested that the two EU instruments are themselves insufficiently clear.

**Again, one way of addressing the problem is through the national DPAs, which, if the GDPR has been fully implemented, will have the power to promote awareness of the data protection rules.** The DPAs could do this either by issuing informal guidance, or by arranging training in accordance with

Article 57 of the GDPR explaining how to deal with AML cases. Alternatively, the DPAs and national Governments together could encourage the development of Codes of Conduct in accordance with Article 40 of the GDPR. As regards encouraging public awareness, again Article 57 of the GDPR specifically provides for DPAs to be able to do this.

**Another way of encouraging better awareness among obliged entities and other stakeholders and their staff is by the appointment of Data Protection Officers (DPOs).** These data protection specialists work independently within organisations to provide in-house advice on data protection. The GDPR requires them to be appointed by all public authorities, except the courts acting in their judicial capacity, and by certain other bodies doing large scale processing of personal data. It is not clear from the reports to what extent DPOs have been appointed in the four countries, but there is clearly potential for them to make a significant contribution to AML within large obliged entities such as banks. Again, staff training could be among their activities. Indeed, one country's report says that in some institutions, even where DPOs had been appointed, staff remained unaware of data protection requirements.

Some of the four countries' reports touched on the question of resources. **It is important to ensure that obliged entities have adequate data protection resources in their AML activities**. One way of helping to achieve this, at least for the larger entities, would be by the appointment of DPOs as mentioned above. It is also necessary to ensure that DPAs and other public sector AML supervisors have sufficient funds and are sufficiently well staffed to be to carry out their AML work effectively. One report notes the relatively low number of staff available to the DPA. Depending upon the arrangements for funding independent bodies such as DPAs in the four countries, this will be a matter for national Governments. **Within the limits imposed by the availability of resources, there may well be a case for appointing an AML specialist within each country's DPA.**

Finally in this section there is the question of communications. At least one report mentioned the difficulties caused by the incompatibility of electronic systems. **While the inability of different systems to "speak" to each other can be seen as enhancing the security of personal data since the data are less readily transmissible, it clearly greatly hinders the effectiveness of AML**. What is needed are efficient systems that are interoperable and at the same time provide a high level of security. Such systems come within the scope of Article 25 of the GDPR which requires personal data processing systems to be established in such a way as to protect personal data "by design and by default".

## XIII. INTERNATIONAL CO-OPERATION

This paper describes above the position on the relationship between AML and DP within the EU Member States. **It is clear that Member States have yet to establish coherent working practices that are effective across the whole range of AML activities. More needs to be done, and in the four countries the standards expected should not be higher than those which apply in the Member States themselves.** That said, as the Member States' understanding and implementation of the requirements improves, it is to be hoped that the four countries will be able to learn from their experience and bring their own practice more closely into line with the best standards within the EU. To some extent, the four countries are particularly well placed to receive an early benefit from EU working practices as they develop, due to their fruitful co-operation with numerous EU stakeholders, such as, in particular, through twinning projects as well as other support, which should bring developments into the countries as they emerge.

## XIV. ANALYSIS OF THE 6 CATEGORIES OF AMLD SUBJECTS IN TABLE ABOVE

The content and structure of this section follows the categories used above and combines them with the analysis of the information from the discussions, documents and questionnaires received. In the following, the categories are grouped by preventive and other, for logical reading flow.

Preventive: Private sector bodies / Supervisory bodies / Holders of Registers

Other: Financial Intelligence Units (FIUs) / Law enforcement bodies /Courts

## XV. PRIVATE SECTOR BODIES – OBLIGED ENTITIES IN AMLD

Obliged entities, under AMLD, carry out the following activities involving data processing:

- Customer due diligence (including enhanced and simplified due diligence);
- Transaction monitoring;
- Behavioural monitoring;
- Internal data sharing (including within a group);
- External data sharing (including with regulators and other financial institutions);
- Data sharing for outsourced arrangements; and
- Cross-border processing of data (especially for the processing of international payments)

The Financial Sector is the largest group of obliged entities, and processes the most data, as all clients and all business fall under these requirements. In general, these obligations are established for a long time, are regulated in Law and in subordinate legislation, guidance and established practice by the prudential supervisors. Internal and external audit reviews the application of the rules and ensures improvements over time. Sophisticated IT systems are in use, which means that processing is secure, as a rule.

### A few areas remain sensitive, in the 4 countries reviewed:

**Not all parts of identification and verification of clients, owners, appointed persons and beneficial owners, and of keeping such information up to date, are covered in Law sufficiently in detail in all countries**. This leads to small gaps that clients object to, obliged entities may not fully implement, and supervisors may penalize. Finally, there may be disagreement with DPAs on the need for some of the data. All this should be addressed as it creates a lot of unnecessary friction in the day-to-day application of both sets of rules.

Information of clients about all steps of processing their data is a challenge to all mass market entities, and therefore may be difficult – especially when it concerns beneficial owners, who may be a few layers removed from the client itself.

**Since the 4th AMLD in 2015, there has been a stricter right of deletion explicitly for AML/CFT relevant client data, and obliged entities are required to have adequate programs in place.** As the right to deletion starts 5 years after the end of a business relationship, the practice of this new requirement has not yet been really tested in any larger way. At the end of those five years, the data may be retained for a maximum of five more years in accordance with national DP law but only

where there has been a thorough assessment of the necessity and proportionality of retaining the data for AML/CFT purposes. This will lead to new challenges for IT tools and persons responsible for data protection within entities. **Supervisors would be well advised to develop a strategy covering these topics in close co-operation with the DPA**.

**Data sharing outside the entity, be it with all relevant authorities, with group entities, or with other financial institutions, is exposed to some risks and lack of clarity or limitation**:

- the risk of sharing too much data, for example sharing of other clients' or other accounts' data because they are connected to the specific case,
- the risk of authorities requesting data that go beyond what is necessary – interviews mention pressure by FIU or law enforcement on the private sector,
- the specific risks of sharing data related to tax, as tax irregularities are not all covered under AML regimes, though Tax Authorities are often extremely interested in such data and may pressure obliged entities – or incite the FIU - to provide information beyond the legal requirement, such a situation was mentioned by one of the four countries.

Outside the financial sector, obliged entities include among others lawyers, accountants, real estate agents, jewelers, high value goods dealers and gambling service providers such as casinos and betting shops.

- For big international accountancy firms, and legal firms, the fulfillment of the requirements above is easily within their means. They also – regularly – challenge any excessive application of the AML framework to their work and often do this successfully.
- However, many of the smaller entities and practitioners are very challenged by the AML/CFT requirements and have a less strong grasp of DP.

As already mentioned in the general comments, some lack of awareness and understanding was mentioned in all 4 countries' reports. Professional Bodies and industry representatives have an important role in transmitting information and developing training and guidance. DPAs should support them in these efforts.

## XVI. SUPERVISORY BODIES

## XVII. SUPERVISORS IN THEIR CORE FUNCTION

Supervisory bodies, are mostly tasked with prudential licensing and ongoing supervision of legal entities such as banks, insurance companies, and other financial institutions, including for AML/CFT. These supervisors, as well as other authorities designated under AML/CFT Laws, i.e. a Gaming Commission, also oversee other businesses, so called DNFBPs, (designated non-financial businesses and professions), who are also obliged entities under the AML Directive.

The supervisor's focus is on the lawful activity of the supervised entity, controlling whether and how the obliged entity follows all relevant financial sector laws and regulations, including AML/CFT. Therefore, these supervisory bodies only process individuals' data in limited circumstances, for example, when they review a sample of customer data in their review of accounts, procedures and practices.

The activities concerned are clearly regulated in laws delineating their responsibilities powers and duties. Thus, supervisors have a legal basis which is determined and detailed enough for their actions

when it comes to data processing, allowing them to fulfill the DP requirements mentioned above.

In the responses from the four countries, no major mishandling / abuse of personal data was mentioned, and supervisors' processes related to DP seem robust in practice, based on general confidentiality and careful handling of data deriving from their core laws and duties. However, there seem to be no known explicit data protection procedures and processes in supervisors related to involvement in AML/CFT cases, for example in their own co-operation and reporting to FIU, in assisting in investigations and enforcement actions where applicable, and in case of publication of supervisory enforcement actions.

Overall, while handling of data protection by supervisors might profit from more DP specific attention and documentation, there seem to be no specific DP concerns or problems related to supervisors. While improvements would be welcome on the items mentioned above, a priority need to address specific gaps has not been identified.

## XVIII. SUPERVISORS GUIDING THEIR SUPERVISED ENTITIES

Supervisors increasingly require their supervised entities to provide them with reports about their risk management, about their data management, about their IT use, about contingency planning other general procedures and processes, as well as tools, and outsourcing agreements used by the entity. From this, the supervisor's duty to review an entity's documents and react to potential breaches of the legal framework is usually inferred. As regards DP, this might indicate a responsibility of supervisors for correct handling of data by supervised entities. **Supervisors might wish to review how best to meet these evolving challenges, for example by discussing with national DPAs and defining a clear responsibility and congruent process for advising OEs on DP, and defining the boundaries between their supervisory powers and duties and the formal powers and duties of the DPA.**

## XIX. NOTE ON FIU AS SUPERVISOR

In some instances, the FIU is designated by the national AML Law as the supervisor for AML/CFT. In such a case, a clear demarcation in law, in internal regulation/ guidance and processes between the FIU as supervisor or oversight body, and the FIU in its duties concerned with the analysis and dissemination of suspicious transaction reports needs to be ensured when it comes to data processing, in addition to the points made above. As this need for a clear-cut organisational demarcation line seems to be in place and well understood, nothing further needs to be said.

## XIX. HOLDERS OF REGISTERS

National data protection law, including the special provisions from the AMLD, apply to the processing of personal data held in registers, such as Company Registers, Account Registers and Beneficial Owner Registers. Some countries also have registers of Politically Exposed Persons (PEPs), or some databases of declarations of wealth and income for members of the Government, Parliamentarians and similar top-ranking public figures. It should be borne in mind that some registers, such as registers of PEPs or registers of income and wealth of parliamentarians may, give an indication of political affiliation.

Where that is the case the special rules on the processing of sensitive data are likely to apply.

Increasingly, registers are used by obliged entities online in database-sourced searches to create an AML risk profile for a customer, or to update parts of their client files via special IT tools. This use is in line with the general purpose of registers and does not create new DP issues. Practical application of the requirements of the GDPR to the registers in use in each country might be reviewed and controlled.

## XX. FINANCIAL INTELLIGENCE UNITS (FIUS)

Financial Intelligence Units have been created in most countries as a specialized body in the prevention and detection of Money Laundering and Terrorism Financing. Depending on the Law that creates them, and their affiliation, either as a police FIU or as an administrative FIU, FIUs are covered either by the LED or by the GDPR, in carrying out their official functions. However, the data protection principles established by the LED and its other main requirements are broadly similar to those in the GDPR so all FIUs are subject to equivalent data protection rules. They are independent, and have special tailor-made powers and responsibilities based on the international standards, and their participation in the global organization for FIUs, Egmont Group.

The FIU has been created to

- act as a filter between obliged entities reporting as per above (transactions that are "large, complex and unusual" or "without clear economic purpose" and clients whose actual identity and source of funds/ wealth cannot be ascertained) and criminal investigative bodies, nationally and internationally,
- act as an analysis and enrichment unit with access to restricted databases of many authorities (customs, police, car registrations, passports, cadastral register, company register, …the list varies)
- as a hub for cooperation and investigation, collecting data from and cooperating with obliged entities, national law enforcement and supervisors as well as international FIU and law enforcement, on issues related to illicit financial flows, suspected financial crime, and predicate offences,
- and in some cases, FIU is itself a supervisor for some entities related to their preventive actions on AML/CFT.

Concerns with the data protection within /connected to FIU come from all 4 countries in varying intensity and have led to some important good practice.

## XXI. LAW ENFORCEMENT BODIES, PROSECUTORS AND COURTS

**It is probably in the law enforcement field that the need for a careful balance to be struck between AMLD and DP comes out most strongly.** Where they identify cases which they suspect may come within the AMLD, the police and other law enforcement agencies as well as the prosecutors have the duty to take the action required by their professional obligations. This can mean pursuing in the public interest cases which involve large quantities of personal data, some of which may be sensitive. On the other hand, the mere fact that an action is, or is claimed to be, in the public

interest is not a sufficient ground for overriding the data protection rules. The application of certain provisions (but not all) of data protection law can be restricted, but only where the restriction "... constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests..." of the individuals concerned, in order to safeguard important specified interests. These interests include the prevention, detection, investigation or prosecution of criminal offences. This formulation, which is taken from Article 15.1 of the LED, has its ultimate origins in Article 8 of the European Convention on Human Rights, which provides for the right to private life.

**When they are carrying out their official functions, law enforcement bodies such as prosecutors, the police and the courts dealing with criminal cases are subject to the LED rather than the GDPR.** One country's report suggests that there is good practice by the police. On the other hand, another report suggests that there is a lack of efficiency on the part of judges, prosecutors and law enforcement agencies in implementing the legislation, and that this leads to a lack of both legal certainty and concrete results. Other countries' reports suggest that awareness is low among law enforcement bodies and identify a strong need for training on both AML and DP for prosecutors and judges. One report recommends the establishment of a data protection specialist in the prosecutor's office. Another says that while there was already a data protection specialist in the Prosecutorial Council, that specialist's remit did not extend to individual prosecution offices. That country's report goes on to say that judges and prosecutors find difficulty in dealing with AML cases because of the highly technical issues involved. The interviewee in question said that the legal training available in the country did not cover AML. He/she went as far as suggesting that, perhaps as a consequence of that, the issue was not seen as being important.

As noted above, Montenegro's report lists all the bodies which have signed an agreement in the field of crime prevention. The agreement provides for automatic data exchange between all institutions including the revenue administration (taxes, customs and games of chance) and data from the real estate administration. The agreement states precisely what information may be exchanged and in what way. It also contains provisions on the mandatory protection of personal data during data processing and exchange. The report does not say whether or not the DPA was consulted during the preparation of the agreement, which would have been desirable, but nonetheless this is an example of good practice that could usefully be followed in other countries.

The overall picture therefore is mixed, with some countries seeming to be coping well in the law enforcement field, while others recognise that there is a need for improvement, particularly as regards awareness, written procedures, processes in practice, and training. DPOs, who are required to be appointed by all the relevant agencies, except courts acting in their judicial capacity, can help with this.

## XXII. RECOMMENDATIONS AND CONCLUSIONS

Both AML/CFT and DP are very dynamic areas of legislation and institutional development, both in EU and in the four countries in this report. This means that hard work in all the countries concerned leads to rapid change in the legal framework that is described in the reports on each individual country. The recommendations in this paper draw broad lines on overarching themes at the juncture of AML and DP that should prove useful on the road moving forward.

While it may not match the most recent EU requirements all countries have a DP framework in place, as well as an AML/CFT framework, that broadly covers relevant issues while being upgraded and

updated. This is mostly parallel to developments in EU countries, where transpositions of the topics are ongoing, and complex with some gaps being addressed more slowly. This report focuses on a few general ideas.

## XXIII. RECOMMENDATIONS

- **Broad awareness raising and alignment through outreach and connection building is needed so that both topics get the necessary attention**

  The core authorities and responsible topical stakeholders are aware of the current developments, and have either created the legal and institutional measures needed, or are working at doing so. However, some of the authorities are only aware of their own areas of responsibility and lack awareness and willingness to include either AML or DP as an area of concern in their planning and activity. DPAs can help with this through the provision of informal guidance and formal training and the development of Codes of Conduct and public awareness raising activities. The appointment of DPOs is also an important way of helping achieve better understanding within organisations. DPOs should liaise closely with the national DPA.

- **Data Protection Authorities must be fully operational and active in AML/CFT matters**

  Data Protection Authorities are not yet actively present in all aspects of AML/CFT in all countries Some DPAs are still in the stage of becoming fully operational. Others are not focusing on AML/CFT. In one case, although the national law provides for a DPA, the post has not yet been filled. This must be done as a matter of urgency.
  Given the pivotal role that DPAs play in ensuring data protection and the strong need for advice, help and support on data protection among AML/CFT stakeholders, subject to the availability of adequate finance, there may well be a case for DPAs to appoint an AML specialist.

- **Dialogue between all Public Sector Bodies responsible in this area**

  The authorities identified in the table, and further described in the six categories should engage in active dialogue with the DPA, ideally in a recurring format such as a Working Group or Committee focusing on the topics identified here and any other issues arising in the implementation of AML/CFT and of DP developments down the line.

- **Inter-agency dialogue should result in output that supports the private sector in fulfilling their legal obligations both for AML/CFT and DP**

  This could be active dialogue, awareness raising, outreach with the and the overviews achieved in this exercise will assist in ensuring DPAs interfacing at a strategic level with AML/CFT authorities on all aspects. DPAs should be centrally involved in the provision of training, outreach, and awareness-raising, also showing publicly interest and awareness of the AML/CFT challenges.

- **DPOs should be appointed where required by law, and to the extent that resources permit in other cases**

  DPOs should be appointed wherever such an obligation exists. DPAs should help organisations with the appointment of DPOs and support DPOs to enable them to be fully cognizant of the AML/CFT issues, and involved in the provision of training, outreach, and awareness-raising in particular obliged entities. Within public bodies, and, where they have been appointed, by obliged entities, DPOs should be in lively cooperation with DPAs.

- **There should be written procedures, processes and guidance (in particular "standard operating procedures") in all authorities and in all inter-authority cooperation where data are concerned**

  The pervasive view that where information travels on paper, the existing approaches either do not touch upon data protection, or safeguard modern data processing anyway, creates a regrettable gap in understanding and instruction covering "all hands through which data are passing". Again, DPOs should be involved.

- **Particular support and attentions should be given to the FIU where many AML/CFT and DP topics converge**

  Countries should ensure that that FIU is aware of its special role also when it comes to DP, and ideally assists other authorities in fulfilling DP requirements in AML/CFT. Cooperation on DP with EU FIUs would benefit all FIUs, and strengthen both the national work and the international FIU cooperation that is a linchpin of FIU work.

- **Obliged Entities should receive support in managing their dual obligations for AML/CFT and DP**

  In particular:

  - Awareness raising, guidance, training and outreach from the DPA, their supervisors and from the FIU that specifically addresses the interface between DP and AML/CFT and gives obliged entities the comfort that they lawfully in both areas.
  - All data processing by obliged entities would profit from a close alignment between Supervisors and the DPA resulting in a written output such as guidelines or best practice papers.

- **National DPAs and AML/CFT responsible authorities should work together to promote a good understanding of the interface between AML/CFT and DP which should allow personal data to be properly protected, and permit the identification of the most sensitive areas in order to seek proper solutions**

  An understandable bias towards fighting the scourge of corruption, organized crime and illicit financial flows appears to lead to less effort being made in aligning with data protection, especially where it comes to mass processing of ordinary people's data. The most sensitive areas are:

  - **Long term data collection, storage and profiling / monitoring in obliged entities**, in particular banks who have by far the largest and most complete data sets on all their customers.
  - **Suspicious Transaction / Activity Reports to FIU** which from the side of obliged entities in the largest part of cases constitute reports of "large, complex, unusual transaction", of business that has "no apparent economic purpose", and of clients (& beneficial owners) whose identity cannot be fully clarified and documented. Handling these reports, processing their data and data retention in FIU, as well as national and international cooperation related to such data, are the most sensitive area as far as – in the largest part of cases - fully legitimate activity and ordinary people are concerned.
  - Protecting legitimate rights of individuals whenever **publication of AML/CFT relevant report**s occurs, in view of personal data protection.

- **Relations with the EU**

  As the Member States' understanding and implementation of the requirements improves, the four countries will be able to learn from their experience and bring their own practice more closely into line with the best standards within the EU. They are particularly well

placed to benefit from EU working practices as they develop through co-operation with numerous EU stakeholders, such as twinning projects.

- **Laws on Supervision, which cover general confidentiality rules, and established processes in Supervisors who deal mostly with aggregate data, would indicate this area to be less exposed to DP weaknesses**

There is a need within supervisory bodies for clear procedures and processes in dealing with data protection matters.
Overall, while most supervisors might profit from AML/CFT specific internal guidelines or best practice papers, the general confidentiality rules and processes governing their work cover the needs of DP to a large extent. Further, the impact of supervisory bodies themselves is limited when it comes to their risk of inappropriately processing personal data in the context of AML/CFT, as they mostly work with aggregate data. With scarce resources, based on cost/ benefit views, the priorities of the 4 countries might most profitably lie elsewhere for now.

- **There is a need for greater interoperability between all IT systems involved in this topic**

This may need a longer-term approach due to the overall complexity and cost. As a minimum, it would be essential to include interoperability aspects whenever upgrading or creating relevant IT systems in the four countries, in order to create and/or connect IT systems in such a way that, over time, secure exchange of data becomes the default option, between all players in the AML/CFT arena.

  - On a positive note:

    One essential element is in place in most countries already and should help align DP and AML/CFT as to IT systems:
    Most FIUs use the GoAML reporting system (developed and updated by UNODC) which has become the international standard. Any improvements in data processing in UNODC updates of this system will lead to improvements for all countries using this system for their reporting channels between FIUs and obliged entities, at a nearly global scale.

- **Law enforcement**

Overall, awareness about the relationship between AML and data protection appears to be low among law enforcement bodies and there is a strong need for training on both AML and DP for prosecutors and judges.

## XXIV. CONCLUSIONS

The four countries could markedly improve their effectiveness in protecting data of individuals while continuing an effective fight against ML/FT if they were to

- **engage in communication and coordination of public bodies such as DPA, FIU and Supervisors on the interface of the two topics,**
- **ensure expertise on both sides to take into account the interests of the other in the work they do,**
- **and provide all stakeholders and the public with some clear messages, broad guidelines, clear definitions and demarcation lines and training - as well as ongoing dialogue.**

The building blocks seem to be there, there is growing awareness among some of the stakeholders,

there is some dialogue in place that might accommodate this agenda, a foundation exists. Where there is a will at senior level, the topic might be included in activities going on anyway. This would bring knowledge and clarity about areas of common concern among persons who need to include some space in their own strategies and projects for the respective “other angle”. In the context of many workstreams driven by becoming closer to the EU, the authorities are currently evolving because of various reforms coming up, and the legal framework is in flux for the same reason - so the moment is good to create the links needed in law, and in public bodies.

In smaller countries, where senior officials meet often, and informal and rapid communication happens all the time, a rapid change of awareness for all stakeholders could happen fast - many of the reported problems seem to lie in not enough attention for the intersection of AML/CFT and DP in its various forms and applications.

This is no way negates the many detailed challenges that would remain, but it would bring the quick and easy wins to the forefront and allow for palpable improvements.

**This possibility could be a cause for optimism.**

# XXV. Annexes

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

TRANSPARENCY INTERNATIONAL MACEDONIA

# FIGHT MONEY LAUNDERING WITH PERSONAL DATA PROTECTION IN MACEDONIA

**Prof. Elena Andreevska**
**Ph.D Slagjana Taseva**

**May 2021**
**Skopje, Republic of North Macedonia**

Acronyms

General Data Protection Regulation (GDPR)

Organization for Economic Co-operation and Development (OECD)

Council of Europe (CoE)

European Union (EU)

The European Union Agency for Fundamental Rights (FRA)

Law Enforcement Authorities (LEAs)

Law on Personal Data Protection (LPDP)

# INTRODUCTION

By the end of the 1970s, two important international organizations started to prepare international instruments on the processing of information about individuals: the Organization for Economic Co-operation and Development (OECD) and the Council of Europe. Their early involvement, and examines in detail how OECD's 1980 Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data,[1] on the one hand, and Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[2] on the other, marked crucial steps in the evolution of the terms 'data protection' and 'privacy' in Europe. It shows that this institutionalized international cooperation resulted in the labeling of all existing and upcoming European rules on the processing of data as concerned with 'data protection', as well as in their progressive linkage with the word 'privacy'. The embroilment between these expressions was later transferred into European Union (EU) law, and is instrumental to understand the emergence of the EU fundamental right to the protection of personal data.

Article 8 of the EU Charter of Fundamental Rights[3] guarantees individuals' fundamental right to the protection of personal data. Article 8 also entails the key data protection principles associated with this fundamental right. The processing of personal data must be fair, for specified purposes, and based on either the consent of the person concerned or a legitimate basis laid down by law. Individuals must have the right to access their personal data and to have it rectified, and compliance with this right must be subject to control by an independent authority.[4]

Since 25 May 2018, the General Data Protection Regulation (GDPR) has applied across the 28 EU Member States. It provides a single set of data protection rules applicable in each EU Member State, thereby harmonizing the implementation of the right to data protection across the EU. The GDPR benefits both businesses and individuals by establishing an environment of legal certainty. The GDPR preserves and develops the core rights and principles set out in the 1995 Data Protection Directive.[5] It also introduces new obligations for entities that process personal data. For instance, it requires the implementation of data protection by design and by default; it stipulates that a data protection officer must be appointed in certain circumstances; it establishes a new right to data portability and it also stipulates that entities must comply with the principle of accountability. In addition, the regulation introduces a number of procedural safeguards that oblige entities that deal with personal data to better inform individuals, to refrain from unnecessary or disproportionate use of personal data and to increase the security of stored data. These safeguards aim to better protect personal data with respect to their processing, but, nevertheless, may appear complex or burdensome for smaller and/or non-expert organizations, including some civil society organizations (CSOs). [6]

1 These Guidelines were updated in 2013. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD.

2 Convention 108. In addition, the Council of Europe has adopted a number of recommendations aimed at applying the general principles set out in the convention to the specific requirements of various areas of society: Protection of health-related data (2019); Guidelines to respect, protect and fulfill the rights of the child in the digital environment (2018); The roles and responsibilities of internet intermediaries (2018); The processing of personal health-related data for insurance purposes, including data resulting from genetic tests (2016); Protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality (2016); The processing of personal data in the context of employment (2015); a Guide to human rights for Internet users (2014); Protection of human rights with regard to social networking services (2013); Protection of human rights with regard to search engines (2013); Profiling (2010); On the protection of personal data collected and processed for insurance purposes (2002); Privacy on the Internet (1999); Personal data collected and processed for statistical purposes (1997); Medical and genetic data (1997); Personal data in the area of telecommunication services, telephone in particular (1995); Communication to third parties of personal data held by public bodies (1991); Data used for employment purposes (1989); Police files (1987); Social security (1986); Direct marketing (1985); Scientific research and analysis (1983); Automated medical data banks (1981).

3 See Official Journal of European Union, C 326/392, 26.10.2012.

4 The European Union Agency for Fundamental Rights (FRA), together with the Council of Europe and the European Data Protection Supervisor, published a handbook on European data protection law, which explores the application of this right in more detail, Luxembourg: Publications Office of the European Union, 2018.

5 Directive 95/46/EC.

6 See FRA et al. (2018); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016.

# 1. 4TH AND 5TH EU MONEY LAUNDERING DIRECTIVE

Regulation (EU) 2016/679 of the European Parliament and of the Council,[7] the European Union's ('EU') new General Data Protection Regulation ('GDPR'), regulates the processing by an **individual, a company or an organization** of **personal data** relating to **individuals** in the EU. It doesn't apply to the processing of personal data of deceased persons or of legal persons.

The rules don't apply to data processed by an individual for purely personal reasons or for activities carried out in one's home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, for example, then the data protection law has to be respected.

Alongside the GDPR, the Reform encompassed a Directive establishing rules for the protection of individuals with regard to the processing of personal data by competent authorities for purposes of law enforcement (LED).[8] The LED put forth great achievements in areas that had previously not been regulated by EU law. Therefore, the LED constitutes a major step forward in establishing a comprehensive EU data protection regime, as the first horizontal and legally binding instrument laying down the rules for national and cross-border processing of personal data in the area of law enforcement.

Although the LED received way less attention than the GDPR, two main objectives of the Directive are too important to be neglected: the increased level of fundamental rights protection in the area of police and criminal justice, and the improved sharing of personal data between the Member States, as they will be able to rely on uniform data protection rules.

The LED is a modern instrument, designed for the processing of personal data by Law Enforcement Authorities (LEAs) in the Digital Age, which is why there is no doubt that instruments such as the Directive are rapidly gaining in importance and visibility: firstly, an increased number of criminal acts is being committed online or with the help of online tools. Perpetrators of crime leave digital traces that may support LEAs in their tasks of crime prevention detection, investigation and prosecution.

Secondly, as perpetrators are becoming more tech-savvy, LEAs turned to new investigative techniques, including big data analytics. The term big data police technologies may include predictive systems that identify people or places suspected of crime, surveillance systems to monitor at-risk areas and search systems to mine data for investigative clues or to develop intelligence nets of helpful data for groups or across communities.

Thirdly, EU rules on the processing of personal data by LEAs are undergoing consolidation, with the LED acting as a locomotive.

The rules of the LED, which had to be transposed into the national laws of all 28 Member States and the four Schengen Area States (Norway, Iceland, Switzerland and Lichtenstein) by 6 May 2018, benefited from the attention given to the GDPR, as some of the Regulation's solutions could simply be taken over. However, a number of provisions were developed specifically for the personal LED.

## 1.1. What's changed?

Core aspects from the 3rd EU Money Laundering Directive remain unchanged, such as record keeping, verification of businesses and people, and the establishment of beneficial ownership. The new Directive does, however, implement the following changes:

[7] See the Official Journal of the European Union, 5.6 2015.

[8] **(EU) 2016/680.directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.**

- **Risk assessments:** Every financially regulated organization must have written and documented Anti Money Laundering/Counter Terrorism Financing (AML/CTF) risk assessments, policies and procedures. They must have a process which has been tested to assess their effectiveness and implementation, which is proportionate to the size of the organization.
- **Enhanced due diligence:** The definition of a Politically Exposed Person (PEP) is being enhanced: - organizations will now need to consider if a beneficial owner is a PEP - people with high level appointments.[9]
- **Beneficial ownership:** There is a new requirement for all companies, legal entities and trustees to hold adequate, accurate and up-to-date information on their beneficial owners. They are also required to make this available to those involved in AML/CTF due diligence and law enforcement agencies.
- **Simplified due diligence:** Simplified due diligence provisions are no longer specifically contained in the 4th Directive, although individual countries may permit simplification following an evidence-based assessment within their jurisdiction.
- **Record keeping:** Further clarity around record keeping requirements is included to attempt to make them more consistent with the requirements of the data protection legislation.

## 1.2. What are the implications?

While the new directive attempts to provide clarity on some areas of the 3rd Directive, it raises additional issues. For example: Simplified due diligence; Record keeping; Beneficial ownership; and Risk assessment.

**GDPR fines are designed to make non-compliance a costly mistake for both large and small businesses.**

The European Union's GDPR was designed to apply to all types of businesses, from multi-nationals down to micro-enterprises. The fines imposed by the GDPR under Article 83 are flexible and scale with the firm. Any organization that is not GDPR compliant, regardless of its size, faces a significant liability.

## 1.3. Controllers and processors:

Organizations that collect and control data (controllers) and those that are contracted to process data (processors) must adhere to rules governing data protection, lawful basis for processing, and more.[10]

**Certification bodies:** Accredited bodies charged with certifying organizations must execute their evaluations and assessments without bias and via a transparent process.[11]

**Monitoring bodies:** Bodies that have been designated to have the appropriate level of expertise must demonstrate independence and follow established procedure in handling complaints or reported infringements in an impartial and transparent manner.[12]

**The basic principles for processing:** Data processing must be done in a lawful, fair, and transparent manner. It has to be collected and processed for a specific purpose, be kept accurate and up to date, and processed in a manner that ensures its security. Organizations are only allowed to process data if they meet one of the six lawful bases listed in Article 6. In addition, certain types of personal

[9] In the UK will now be PEPs - enhanced measures will need to apply for at least 18 months (rather than the former 12) after a PEP leaves office.
[10] Articles 8, 11, 25-39, 42, and 43.
[11] Articles 42 and 43.
[12] Article 41.

data, including racial origin, political opinions, religious beliefs, trade union membership, sexual orientation, and health or biometric data are prohibited except under specific circumstances.[13]

**The conditions for consent**: When an organization's data processing is justified based on the person's consent, that organization needs to have the documentation to prove it.[14]

**The data subjects' rights**: Individuals have a right to know what data an organization is collecting and what they are doing with it. They also have a right to obtain a copy of the data collected, to have this data corrected, and in certain cases, the right to have this data be erased. People also have a right to transfer their data to another organization.[15]

**The transfer of data to an international organization or a recipient in a third country**: Before an organization transfers any personal data to a third country or international organization, the European Commission must decide that that country or organization ensures an adequate level of protection. The transfers themselves must be safeguarded.[16] They also include, any violation of member state laws adopted under Chapter IX.

**Non-compliance with an order by a supervisory authority**: If an organization fails to comply with an order from the monitoring bodies of the GDPR, they have set themselves up to face a huge fine, regardless of what the original infringement was. And these are just the administrative fines.[17]

## 1.4. How much is a GDPR fine?

Under the GDPR, fines are administered by the data protection regulator in each EU country. That authority will determine whether an infringement has occurred and the severity of the penalty. They will use the following 10 criteria to determine whether a fine will be assessed and in what amount:

- **Gravity and nature:** The overall picture of the infringement. What happened, how it happened, why it happened, the number of people affected, the damage they suffered, and how long it took to resolve.
- **Intention:** Whether the infringement was intentional or the result of negligence.
- **Mitigation:** Whether the firm took any actions to mitigate the damage suffered by people affected by the infringement.
- **Precautionary measures:** The amount of technical and organizational preparation the firm had previously implemented to be in compliance with the GDPR.
- **History:** Any relevant previous infringements, including infringements under the Data Protection Directive (not just the GDPR), as well as compliance with past administrative corrective actions under the GDPR.
- **Cooperation:** Whether the firm cooperated with the supervisory authority to discover and remedy the infringement.
- **Data category:** What type of personal data the infringement affects.
- **Notification:** Whether the firm, or a designated third party, proactively reported the infringement to the supervisory authority.
- **Certification:** Whether the firm followed approved codes of conduct or was previously certified.

[13] Articles 5, 6 and 9.
[14] Article 7
[15] Articles 12-22.
[16] Articles 44-49.
[17] Article 82. See also Chapter IX witch grants EU member states the ability to pass additional data protection laws as long as they are in accordance with the GDPR. Any violation of these national laws also faces GDPR administrative fines.

- **Aggravating/mitigating factors:** Any other issues arising from circumstances of the case, including financial benefits gained or losses avoided as a result of the infringement. If regulators determine an organization has multiple GDPR violations, it will only be penalized for the most severe one, provided all the infringements are part of the same processing operation.

Finally, many companies use third parties, like email or cloud storage services, to handle their data. While this can be helpful in adhering to the GDPR if the third party has a higher technological capacity, it does not absolve the hiring organization (i.e. the controller) from ensuring that personal data is processed in accordance with the GDPR. Unless the controller can clearly demonstrate that it was "not in any way responsible for the event giving rise to the damage," it will be fully liable for any infringement caused by a non-compliant third party. For this reason, it's important to carefully vet any third party services you use to make sure they have a good track record for security.

## 1.5. What constitute the data processing?

Processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the **collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination** or otherwise making available, **alignment or combination, restriction, erasure or destruction** of personal data. It should be noted that GDPR applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured system.

## 1.6. What is the personal data?

Personal data is any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified or encrypted but can be used to re-identify a person remains personal data and falls within the scope of the GDPR.

Personal data that has been rendered **anonymous** in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

The GDPR protects personal data **regardless of the technology used for processing that data** – it's technology neutral and applies to both automated and manual processing, provided the data is organized in accordance with pre-defined criteria (for example alphabetical order). It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.[18]

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;
- or the monitoring of their behaviour as far as their behaviour takes place within the Union."[19]

[18] Note that in some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies – the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1).

[19] Article 3 (2). The GDPR in Article 3 details processing by a controller or processor. A "Controller" under GDPR is the organization or company which determines the purposes of the processing of personal data where a "processor" carries out the processing of the personal data on behalf of the "Controller". A "processor" can further engage "sub-processors" and the "Controller" would have visibility and approval rights over these "sub-processors".

## 1.7. What is data controller or data processor?

The **data controller** determines the **purposes** for which and the **means** by which personal data is processed. So, if your company/organization decides 'why' and 'how' the personal data should be processed it is the data controller. Employees processing personal data within your organization do so to fulfil your tasks as data controller.[20]

There is no doubt that such rules are rapidly gaining importance and visibility. There are at least three factors contributing to the allure of previously neglected legal texts: firstly, an increased number of criminal acts is being committed online or with the help of online tools. Perpetrators of crime leave digital traces that may support law enforcement authorities (LEAs) in their tasks of crime prevention, investigation, detection and prosecution. Data collection and data exchanges progressively gained in importance for successful police work. Secondly, as perpetrators are becoming more tech-savvy, LEAs turned to new investigative techniques, including big data analytics. The term big data police technologies may include predictive systems that identify people or places suspected of crime, surveillance systems to monitor at-risk areas and search systems to mine data for investigative clues or to develop intelligence nets of helpful data for groups or across communities. Thirdly, EU rules (both the patchwork of data protection rules adopted under the former third pillar6 and the rules for EU Justice and Home Affairs Agencies) on the processing of personal data by LEAs are undergoing consolidation, with Directive (EU) 2016/6808 (LED) acting as a locomotive. However, very important work in this area was carried out by some academics in the past.[21] Moreover, the LED is a modern instrument, designed for LEAs processing personal data in the Digital Age. However, a number of provisions were developed specifically for the Directive. There is a **joint controller** when together with one or more organizations it jointly determines 'why' and 'how' personal data should be processed. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with the GDPR rules. The main aspects of the arrangement must be communicated to the individuals whose data is being processed.[22]

The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking.

The duties of the processor towards the controller must be specified in a contract or another legal act. For example, the contract must indicate what happens to the personal data once the contract is terminated. A typical activity of processors is offering IT solutions, including cloud storage. The data processor may only sub-contract a part of its task to another processor or appoint a joint processor when it has received prior written authorization from the data controller.

There are situations where an entity can be a data controller, or a data processor, or both.

---

20 Tthere is a lack of research covering regulations for the processing of personal data in the law enforcement sector.

21 In particular, see Franziska Boehm 'Information sharing and data protection in the Area of Freedom, Security and Justice – Towards harmonised data protection principles for EU-internal information exchange', Springer 2012; Paul de Hert, Vagelis Papakonstantinou and Cornelia Riehle 'Data protection in the third pillar: cautious pessimism', in Martin Maik (Editor), Crime, Rights and the EU: The Future of Police and Judicial Cooperation, London, Publisher: Justice, 2008, (196p.) 121-194; Diana Alonso Blas, First pillar and third pillar: need for a common approach on data protection? In: Gutwirth, S., 'Reinventing Data Protection?', pp. 225–237. Springer, Berlin (2009). Also. see: Paul de Hert and Vagelis Papakonstantinou 'Data protection policies in EU Justice and Home Affairs. A multi-layered and yet unexplored territory for legal research', in Ariadna Ripoll Servent & Florian Trauner (eds), Routledge Handbook of Justice and Home Affairs Research, Routledge, London, 2018, 169-179 and Nadia Purtova (2017), 'Between GDPR and the Police Directive: Navigating through the maze of information sharing in Public-Private Partnership', available at SSRN: https://ssrn.com/abstract=2930078. Electronic copy available at: https://ssrn.com/abstract=3285873 Cole/Boehm GDPR Commentary (forthcoming Edward Elgar Publishing, 2019).

22 Chapter IX of the Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018. 8 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

# 2. DATA PROTECTION (EU) 2016/680 FOR POLICE AND CRIMINAL JUSTICE AUTHORITIES: STRUCTURE OF THE DIRECTIVE

Processing of personal data by police and criminal justice authorities was, until recently, not an activity that caught a lot of attention of academia and practitioner.[23] Laws regulating such processing were perceived as dry, technical and fragmented.[24] Furthermore, these are not provisions concerning commercial activities generating income and affecting consumers of services, which was another reason reducing their attractiveness. Although there is a lack of research covering regulations for the processing of personal data in the law enforcement sector, there is no doubt that such rules are rapidly gaining importance and visibility. There are at least three factors[25] contributing to the allure of previously neglected legal texts: firstly, an increased number of criminal acts is being committed online or with the help of online tools. Perpetrators of crime leave digital traces that may support law enforcement authorities (LEAs) in their tasks of crime prevention, investigation, detection and prosecution. Secondly, as perpetrators are becoming more tech-savvy, LEAs turned to new investigative techniques, including big data analytics. The term big data police technologies may include predictive systems that identify people or places suspected of crime, surveillance systems to monitor at-risk areas and search systems to mine data for investigative clues or to develop intelligence nets of helpful data for groups or across communities.[26] Thirdly, EU rules (both the patchwork of data protection rules adopted under the former third pillar[27] and the rules for EU Justice and Home Affairs Agencies[28] on the processing of personal data by LEAs are undergoing consolidation, with Directive (EU) 2016/6808 (LED) acting as a locomotive.[29]

Like the GDPR, the LED was adopted in May 2016, constituting a major step forward in establishing a comprehensive EU data protection regime, as the first horizontal and legally binding instrument laying down the rules for national and cross-border processing of personal data in the area of law enforcement.[30] Moreover, the LED is a modern instrument, designed for LEAs processing personal data in the Digital Age. As the second part of the data protection reform package that had been under discussion for four years, the Directive received way less attention than the GDPR. However, two main

---

23 However, very important work in this area was carried out by some academics in the past. In particular, see Franziska Boehm 'Information sharing and data protection in the Area of Freedom, Security and Justice – Towards harmonized data protection principles for EU-internal information exchange', Springer 2012; Paul de Hert, Vagelis Papakonstantinou and Cornelia Riehle 'Data protection in the third pillar: cautious pessimism', in Martin Maik (Editor), Crime, Rights and the EU: The Future of Police and Judicial Cooperation, London, Publisher: Justice, 2008, (196p.) 121-194; Diana Alonso Blas, First pillar and third pillar: need for a common approach on data protection? In: Gutwirth, S., 'Reinventing Data Protection?', pp. 225–237. Springer, Berlin (2009).

24 See: Paul de Hert and Vagelis Papakonstantinou 'Data protection policies in EU Justice and Home Affairs. A multi-layered and yet unexplored territory for legal research', in Ariadna Ripoll Servent & Florian Trauner (eds), Routledge Handbook of Justice and Home Affairs Research, Routledge, London, 2018, 169-179 and Nadia Purtova (2017), 'Between GDPR and the Police Directive: Navigating through the maze of information sharing in Public-Private Partnership', available at SSRN: https://ssrn.com/abstract=2930078.

25 4 See: Paul de Hert and Juraj Sajfert 'Police, privacy and data protection from a comparative legal perspective" in Monica den Boer (editor), "Comparative policing', Edwar Elgar Publishing, forthcoming in 2018.

26 Andrew Guthrie Ferguson 'The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement', NY: New York University Press, 2017, p.272.

27 According to Article 62(6) of the LED, the instruments such as the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210/1 (6 August 2008), the Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210/12 (6 August 2008), or the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L386/89 (29 December 2006) should be aligned with the LED by 6 May 2019.

28 See Chapter IX of the Regulation (EU) 2018/1725 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, According to Article 62(6) of the LED, the instruments such as the Council Decision 2008/615/JHA of 23 June 2008 on the offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018.

29 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131.

30 See: Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33 (2017), 324-340.

objectives of the Directive are too important to be neglected: the increased level of fundamental rights protection in the area of police and criminal justice, and the improved sharing of personal data between the Member States, as they will be able to rely on uniform data protection rules (Article 1(2)). The Directive is the successor to the 2008 Framework Decision 200811, which had a much more limited scope and solely applied to cross-border data processing between the Member States.

## 2.1. Meandering between the Directive and the GDPR

One of the most important provisions of the Directive is to be found at its very beginning. Article 1(1) defines the scope of the Directive, which is crucial for a clear delineation between the Directive and the GDPR. In order for the Directive to be applicable, both its personal and material scope have to be met. In other words, the processing must be carried out by a competent authority (personal scope) for the purposes of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (material scope).[31]

Whenever a police officer processes data for non-law enforcement purposes, for instance, and as the most obvious example, HR data or information that is to be archived, the GDPR will apply. Yet, in other areas where LEAs may be competent to process personal data, the delineation between the Directive and the GDPR is not as apparent. This might be the case in situations where police officers process personal data for identification or verification purposes in the field of migration and border control.[32] However, once the irregular migrant applies for asylum, the processing of his application will fall within the scope of the GDPR, notwithstanding the initiated criminal proceedings.

In accordance with the above, the Directive should apply only if both the personal and the material scope are satisfied. If one of the two criteria is not met, either the GDPR or other EU[33] instruments will apply, unless the processing is being performed for purposes falling completely out of scope of EU law, in which case none of the EU Regulations/Directives will be applicable (for example, when a military intelligence service is collecting data about persons plotting to threaten the national security of a country by destroying its crucial army bases). Although the legal basis of Article 16 TFEU, on which both the GDPR and the Directive were adopted, is very strong and not a lot of processing activities will fall outside the scope of EU law, the latter does not cover processing carried out by national intelligence and military agencies. This may become problematic where a clear delineation between the different tasks of intelligence agencies is lacking. Therefore, when national intelligence agencies process data for the purposes of the Directive, they should be viewed as competent authorities under Article 2(1) instead of not being covered by EU law. This issue becomes even more relevant in the context of information sharing between national intelligence agencies and LEAs.

## 2.1. Croquis of the Directive

The Directive, just like the GDPR, is divided in ten chapters. Three chapters, I (general provisions), IV (controller and processor) and VI (independent supervisory authorities) are closely linked to the GDPR, incorporating a number of the latter's provisions.

Chapter I reiterates a number of definitions from the GDPR and defines the scope of the Directive, which has been discussed above. It also explains that the Directive is not a full harmonization

[31] Articles 1(1) and 2(1) respectively.

[32] A person crossing the Schengen borders irregularly might be checked by a police officer and, in those Member States where the irregular crossing of borders qualifies as a criminal offence, the police officer may change the purpose of the processing, depending on whether it is carried out for migration purposes or for prosecuting the criminal offence.

[33] For instance, Regulation (EC) No 45/2001 if the processing is carried out by Union institutions, bodies, offices and agencies, or more specific legal regimes, such as the Europol Regulation (EU) 2016/794.

instrument, allowing Member States to introduce higher data protection safeguards from the minimum standards required by the Directive.

Chapter IV, just like the GDPR, introduces the risk-based approach and a number of new obligations for controllers and processors that resemble the ones stipulated in the GDPR (data protection by design and by default, DPIA, notifications of personal data breaches, obligation to appoint a DPO). The Chapter also establishes a duty to keep logs of certain processing operations,[34] which is a specific obligation under the Directive and a very important tool to monitor whether law enforcement databases are used lawfully.

Chapter VI lays down the same requirements as the GDPR regarding the independence of national supervisory authorities and the conditions for the appointment of its members. The Directive leaves it to the Member States whether they establish one supervisory authority competent for the application of both the GDPR and the Directive, or separate supervisory authorities that are responsible for either the Directive or the GDPR. Besides the restriction for the supervisory authorities to supervise courts acting in their judicial capacity (Article 45(2)), Member States may add further independent judicial authorities to be exempted from the administrative supervision of supervisory authorities when acting in their judicial capacity. The latter, optional exemption is designed for national authorities that maintain an equivalent level of independence to that of courts and judges.[35]

Two chapters, VII (co-operation) and VIII (remedies, liability and penalties) endorse several provisions of the GDPR, while omitting the GDPR's provisions on the one-stop-shop, the consistency mechanism, provisions on the dispute resolution by the European Data Protection Board (EDPB), joint operations of the supervisory authorities or the administrative fines under Article 83 of the GDPR. These notable omissions are due to the more basic structure of the Directive, resulting from the Council's anxiousness to keep the supervision of the police and criminal justice authorities within the exclusive remit of the respective national supervisory authority, without the meddling of a supervisory authority from one Member State into another Member State's police work. [36]

Three chapters: II (principles), III (rights of the data subject) and V (international transfers) strongly diverge from their equivalent provisions in the GDPR. They are specifically designed for the needs of LEAs and the particular nature of their processing activities. This is in line with the specificities of data processing by police and criminal justice authorities, recognized in Declaration 21.[37] This is in line with the specificities of data processing by police and criminal justice authorities, recognized in Declaration 2017 attached to the Treaty of Lisbon. On the other hand, those chapters may be perceived as weakening the overall level of protection given to data subjects in EU law and offering too much leeway to police and criminal justice authorities, compared to the remainder of the public sector covered by the GDPR.

In Chapter II, already at the level of principles of processing defined in Article 4 are some important differences compared to the GDPR. Firstly, the Directive does not refer to further processing, but instead introduces the notion of subsequent processing by the same or another controller in paragraphs 2 and In the law enforcement context, such processing is generally deemed compatible with the purposes of the initial data collection.[38] Under the Directive, personal data should be adequate, relevant and not excessive, rather than adequate, relevant and limited to what is necessary, as stipulated under

[34] Article 25.

[35] Cf.: Paul de Hert & Juraj Sajfert, 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data', in: Briere, C. and Weyembergh, A (eds), The needed balances in EU Criminal law: past, present and future, 2017, Hart Publishing, p.250.

[36] Ibid, p. 253.

[37] 'The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.'

[38] The collection was also carried 15 Cf.: Paul de Hert & Juraj Sajfert, 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data', in: Briere, C. and Weyembergh, A (eds), The needed balances in EU Criminal law: past, present and future, 2017, Hart Publishing, p.250. 16 Ibid, p. 253.

Article 5(1)(c) GDPR. Both principles grant more flexibility to LEAs in the performance of their tasks compared to the requirements of the corresponding provisions under the GDPR.

Furthermore, Article 6 introduces a specific obligation for controllers under the Directive to establish a clear distinction between personal data of different categories of data subjects (suspects, convicts, victims, witnesses). The LEAs therefore have to neatly tag and properly organize their databases, in line with the jurisprudence of the ECtHR.[39] Another principle specific to the Directive is laid down in Article 7, requiring personal data based on facts to be distinguished from personal data based on personal assessment. Additionally, the quality, accuracy, completeness and reliability of personal data have to be verified and properly indicated before data exchanges with other authorities may take place. As regards the basis for the lawfulness of processing, the Directive lays down only one legal ground in Article 8 (if necessary for the performance of a task carried out by a competent authority for the purposes of the Directive and based on Union or Member State law), while Article 6 of the GDPR provides for six different legal bases. Obviously, the legislation recognized that LEAs may only carry out tasks permitted by law, and not process data for the purposes of the Directive on the basis of consent, contractual obligations or the controller's legitimate interest.

Article 9 is another very specific provision of the Directive, with two different sets of rules. Firstly, paragraphs 1 and 2 provide the rules for interactions between the Directive and the GDPR. Secondly, paragraphs 3 and 4 authorize specific processing conditions to be attached to transmitted data. These conditions, however, may not be more stringent for the authorities of the receiving Member State than the conditions that are imposed on the authorities of the Member State transmitting the data.[40] With regard to the processing of special categories of data ('sensitive data'), Article 10 of the Directive, unlike Article 9 of the GDPR, does not establish a prohibition in principle. It allows the processing of sensitive data, but only where strictly necessary and subject to appropriate safeguards for the rights and freedoms of the data subjects. These are two important requirements added alongside the general lawfulness requirements pursuant to Article 8. Finally, Article 11 on automated individual decision-making was placed in Chapter II of the Directive instead of Chapter III, where one can find its GDPR equivalent. [41] Apart from this organizational difference, the Article has some distinct features compared to Article 22 GDPR.

Compared to the more 'generalist' Articles of Chapter III of the GDPR, the approach towards data subject rights and their possible limitations under Chapter III of the Directive is circumscribed in more detail, in order to adapt the means of processing personal data to the needs of LEAs. The basic set of rights remains the same (information, access, rectification, erasure, restriction of processing) and those rights may be exercised directly against the data controller. The Directive does not provide for GDPR rights that were primarily designed to be exercised against commercial operators, such as the right to be forgotten or the right to data portability. The controller may limit the right of specific information to be given to the data subject, the right of access and the right to obtain information about the possible refusal of rectification, erasure or restriction of processing in a similar way as under Article 23 GDPR, i.e. if there is a legislative measure allowing for the limitation and if the limitation is necessary and proportionate. The grounds for such limitations are much narrower than under the GDPR and closely linked to the purposes of the Directive. Given that the controllers may limit not only the rights, but also the information about the refusal to grant a certain right, a number of data subjects will receive a neutral reply. It is very difficult, or even impossible, to challenge such replies before courts, as data subjects will not be able to formulate what exactly they are referring to in potential complaints. This is why Article 17 provides for an independent review by the supervisory

[39] See ECtHR App nos 30562/04 and 30566/04 S and Marper v United Kingdom (4 December 2008)2008] .

[40] This is a police cooperation rule introduced in EU law by the so-called Swedish Initiative in 2006 - Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100.

[41] Apart from this organizational difference, the Article has some distinct features compared to Article 22 GDPR.

authority and the exercise of data subject rights indirectly, through the intermediary of the DPA. Finally, Article 18 allows Member States to lay down rules for the exercise of data subject rights in criminal proceedings in accordance with the provisions of the national criminal procedural laws. That means that the Directive is fully applicable to criminal proceedings, but since Member States' criminal procedural codes already provide for rules on information, access, rectification, erasure and restriction of processing, the provision recognizes such codes as correct transposition efforts.

In Chapter V, international transfers shall be allowed, as a general rule, only from one LEA to another and after receiving the authorization of the originating Member State.[42] For example, the French police may transfer personal data received from the German police to the FBI only after receiving the prior authorization of the German authority.[43] As there are no comparable transfer conditions in the GDPR, the provisions on transfers under the Directive may be explained by the Council's and the European Parliament's desire to keep the original controller of operational law enforcement data in control over the use of such data by final recipients. The three-step architecture of conditions for international transfers (adequacy decision - appropriate safeguards - derogations) under the GDPR is replicated in the Directive, but the approach to data transfers by way of appropriate safeguards gives more flexibility to controllers, allowing them to carry out a self-assessment of such safeguards. [44]Finally, chapters IX (implementing acts) and X (final provisions) contain usual and more technical provisions.

It should be notated that Article 39 is a very specific and novel provision providing for, as an exception from the rule, so-called asymmetrical transfers from a LEA in a Member State to private parties in third countries. This Article will be very useful for contacts between EU LEAs and service providers overseas, in particular in the fight against cybercrime and cyber-enabled crime. Finally, chapters IX (implementing acts) and X (final provisions) contain usual and more technical provisions. II. Four focal points of the Directive: profiling, indirect exercise of data subject rights, logs, international transfers The second part of this Chapter will give an overview of four distinct features enshrined in the Directive. Due to the limitations in space and the primary purpose of this commentary to focus 21Articles 13(3), 15(3) and 16(4): Avoid obstructing official or legal inquiries, investigations or procedures; avoid prejudicing the prevention, detection, investigation, or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security; protect the rights and freedoms of others.[45]

## 2.2. Overview of the recent ECHR and European Court of Justice and ECHR case-law related to Data Protection: 2000-2015

The Article 8 encompasses the right to respect for private and family life, home and correspondence. In general, the Court has defined the scope of Article 8 broadly, even when a specific right is not set out in the Article.

In order to invoke Article 8, an applicant must show that his or her complaint falls within at least one of the four interests identified in the Article, namely: private life, family life, home and correspondence.

---

42 According to Article 3 (1) of Regulation (EU) 2018/1725: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;".

43 See France: New Data Protection Law has been adopted: FRANCE: New data protection law has been adopted – Privacy Matters (dlapiper.com).

44 Article 37(1)(b)).

45 See, 30 Cf. Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics', in: Philos. Technol. (2017) 30: 475. From Individual to Group Privacy in Big Data Analytics | SpringerLink; ECtHR App no 47143/06 Roman Zakharov v. Russia (11 December 2015); ECtHR App no 37138/14 Szabò and Vissy v. Hungary (12 January 2016); CJEU C-362/14, Maximilian Schrems, ECLI:EU:C:2015:650; In the fight against cyber-crime, LEAs in the European Union will often perceive the mutual legal assistance channels as being too slow and will have to establish a direct contact with a service provider in a third country (e.g. Microsoft, Apple, Yahoo, Google, Facebook, Twitter etc; and See Paul de Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive', p. 17 and Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33 (2017), 324-340.

Some matters, of course, span more than one interest. First, the Court determines whether the applicant's claim falls within the scope of Article 8. Next, the Court examines whether there has been an interference with that right or whether the State's positive obligations to protect the right have been engaged. Conditions upon which a State may interfere with the enjoyment of a protected right are set out in paragraph 2 of Article 8, namely in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Limitations are allowed if they are "in accordance with the law" or "prescribed by law" and are "necessary in a democratic society" for the protection of one of the objectives set out above. In the assessment of the test of necessity in a democratic society, the Court often needs to balance the applicant's interests protected by Article 8 and a third party's interests protected by other provisions of the Convention and its Protocols.

The primary purpose of Article 8 is to protect against arbitrary interferences with private and family life, home, and correspondence by a public authority.[46] This obligation is of the classic negative kind, described by the Court as the essential object of Article 8.[47] However, Member States also have positive obligations to ensure that Article 8 rights are respected even as between private parties.[48] In particular, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life.[49] These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves,[50] although the principle was first set out in *Marckx v. Belgium*, no. 6833/74.

The principles applicable to assessing a State's positive and negative obligations under the Convention are similar. Regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole, the aims in the second paragraph of Article 8 being of a certain relevance.[51] Where the case concerns a negative obligation, the Court must assess whether the interference was consistent with the requirements of Article 8 paragraph 2, namely in accordance with the law, in pursuit of a legitimate aim, and necessary in a democratic society.

Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such a form or manner that their Article 8 rights may be engaged.[52]

The case law of European Court of Justice in the area of data protection generally interprets the provisions of the Directive 1995/46. The focus is on the exceptions from the prohibition of personal data processing the time period required for data storage, legality of data processing or a cross-border transfer of data.

The group of decisions deals with the exceptions in the protection of personal data. Namely, the Court dealt with the situation, when the Spanish Act enable a processing of personal data without

46 Libert v. France, §§ 40-42.

47 Kroon and Others v. the Netherlands, § 31.

48 Bărbulescu v. Romania [GC], §§ 108-111 as to the actions of a private employer.

49 Lozovyye v. Russia, § 36.

50 See, for example, Evans v. the United Kingdom [GC], § 75.

51 Hämäläinen v. Finland [GC], § 65; Gaskin v. the United Kingdom, § 42; Roche v. the United Kingdom [GC], § 157. Also, see Hämäläinen v. Finland [GC], § 66; X and Y v. the Netherlands, §§ 24 and 27; Christine Goodwin v. the United Kingdom [GC], § 90; v. the United Kingdom, § 71).; (X, Y and Z v. the United Kingdom, § 44; Fretté v. France, § 41; Fretté v. France, § 42; Odièvre v. France [GC], §§ 44-49; Evans v. the United Kingdom [GC], § 77; v. the United Kingdom [GC], § 78; S.H. and Others v. Austria [GC], § 94); Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC]; (no. 931/13, §§ 133 - 138, 27 June 2017).

52 • Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, 27 June 2017; • Mockutė v. Lithuania, no. 66490/09, 27 February 2018; and • Bărbulescu v. Romania [GC], no. 61496/08, 5 September 2017.

subject's consent pursuant to an additional reason, not included in Article 7 of the Directive. It related to data public accessibility.[53]

The Court held that Article 7 of the Directive sets out an exhaustive, restrictive list of cases in which the processing of personal data may be regarded as being lawful. This mast be distinguished from the power of Member States to specify conditions under which the processing of personal data is lawful. However, Member States cannot add new principles relating to the lawfulness of personal data to Article 7 of the Directive or impose additional requirements that have the effect of altering the cope of one of the principles provided for in Article 7.

Moreover, the Court had to analyze a processing of personal data by a central register of foreign nationals.[54] The decision address important concept of necessity as a principle of data protection law. The concept should have its own independent meaning in Community Law. The Court held that the use of Central Register of foreign nationals does not satisfy the requirement of necessity, unless it meets certain characteristics, described in the decision.

The concept of necessity is also analyzed in Joined Cases[55] The Court held that wide disclosure, not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by public authority, but also of the names of the recipients of that income, must satisfy the criteria of the necessity and it must be appropriate. Otherwise, it represents an interference with personal life.

In Joined Cases[56], the Court dealt with the legal clash between data protection law and common agricultural policy. EU regulation of agricultural policy required certain personal data about beneficiaries to be published. However, it represented an interference with their private life. In answering this problem, the Court held that there is no definite answer. In analyses of the possible violation of data protection, the national authorities should draw a distinction based on relevant criteria such as the periods during which those persons have received such aid, the frequency of such aid or the nature and amount thereof.

The Court dealt with the time period required for the storage of information, including personal data. [57] The goal is to find a fair balance between the interest of the data subject in protecting his privacy, in particular his rights to object and bring legal proceedings and the burden which the obligation to store that information represents for the controller. The Court held that Member States have a right to specify a time-limit for storage of information and to provide for access to the information to satisfy the requirement of a fair balance. However, the period of one year did not constitute an excessive burden on the controller.

Also, the Court analyzed the legality of a national legislation, which required an employer to give the national authority responsible for monitoring working conditions an access to records of working time. [58] It held that this activity does not violate Article 6 and 7 of the Directive, provided that this obligation is necessary for the purposes of the performance of the authority.

The Court addressed the nature of the publication of personal data on the internet. It held that it is not possible to presume that the Community legislature intended the expression "transfer of data to a third country" to cover the loading of data by an individual into an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them. [59] Therefore, the publication of personal data does not represent a cross-border transfer of data.

53 C-468/10 and C-469/10.
54 Case C-524/06,
55 C-465/00, C-138/00 and C-139/01.
56 C-92/09 and C-93/09.
57 In Case C-553/07.
58 In Case C-342/12.
59 In Case C 101/01.

Finally, in Case C-131/12 *Google Spain v. AEPD* and *Mario Costeja Gonzalez*, issued on 13 May 2014, the Court of Justice of the European Union made several important pronouncements about EU data protection law, and in particular recognized a right under the EU Data Protection Directive 95/46 for individuals to suppress links generated by Internet search engines (popularly referred to as the "right to be forgotten"). The Court's holdings leave many important questions open, both in regard to technical legal issues and more high-level issues of general jurisprudential and societal importance. The Court also failed to take the significance of the case for the Internet into account. The judgment suffers from the Court's traditionally minimalist style of argument and reluctance to adopt a more open and discursive style. The material and territorial scope of the right to suppress Internet search engine results are potentially much wider than the ability to implement the right effectively, suggesting that a way must be found to define the scope of the right in a way that is proportionate to the ability to implement it, if the judgment is to provide real protection in practice.[60]

It should be noted that one of the European Data Protection Supervisor (EDPS) tasks is to intervene in cases before the Court of Justice of the European Union (CJEU) and the General Court.

There are several ways in which the EDPS can be involved in cases before the Court:

- the EDPS has the power to refer a matter to the Court;
- decisions of the EDPS can be challenged before the Court of Justice; and
- the EDPS may intervene in cases when these are relevant to his tasks.

So far, the EDPS has not brought a case before the CJEU.

Several decisions of the EDPS have been challenged before the Court, but the cases were dismissed or withdrawn at an early stage.[61]

Regulation 45/2001 Article 47(1)(i), which is to be repealed and replaced with a new Regulation which brings it into line with the General Data Protection Regulation, lays down the right of the EDPS to intervene in actions brought before the CJEU.[62]

In practice, this means that the EDPS' right to intervene in court cases is not limited to cases where personal data has been processed by European institutions or bodies, but extends to all matters affecting the protection of personal data, either on EU or Member State level.

The right to intervene extends to the General Court.

The word actions has been interpreted to exclude preliminary ruling proceedings under the Treaty on the Functioning of the EU[63] as well as requests for Opinions. ([64]). To plug this gap, the Court has invited the EDPS to answer questions or provide information on the basis of Article 24 of its Statute on several occasions.

As privacy is a dynamic concept that evolves through litigation and Court decisions, the EDPS closely monitors the case law of the Court of Justice of the European Union and of the European Court of Human Rights.[65]

---

60 Kuner, Christopher, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines (September 15, 2014). Final version published as "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges", in: Burkhard Hess and Cristina M. Mariottini (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55 , LSE Legal Studies Working Paper No. 3/2015, Available at SSRN: https://ssrn.com/abstract=2496060 or http://dx.doi.org/10.2139/ssrn.2496060

61 For instance, Case T-164/09 and T-237/16.

62 In its_orders of 17 March 2005 in the so-called PNR-cases, the CJEU decided that the right of the EDPS to intervene extends to all matters concerning the processing of personal data.

63 Article 267 TFEU.

64 Article 218(11) TFEU.

65 The EDPS sometimes produces summaries of the relevant case-law of these Courts and of national Courts of EU Member States. Also, see Case Law Overview 1 December 2014 - 31 December 2015, Working Document, Relevant case-law of CJEU, ECHR and national courts of EU Member States on the right to the protection of personal data, the right to the protection of private life, access to documents and the right to freedom of expression. Includes reference to pending cases. European Data Protection Supervisor 15 March 2016.

The new EU data protection framework consists of much more than just the GDPR. New rules for the EU institutions and ePrivacy are yet to be finalized, and remain a key focal point for EDPS work. As well as providing advice to the legislator on these new rules, the EDPS has started working with the EU institutions and bodies to prepare them for the changes to come. A particular focus of his efforts in 2016 was on promoting accountability, a central pillar of the GDPR which it is safe to assume will also be integrated into the new rules for EU institutions and bodies.

In 2016, the EDPS also made a considerable effort to help move the global debate on data protection and privacy forward and mainstream data protection into international policies. He advised the EU legislator on the *Umbrella agreement* and the Privacy Shield and engaged with data protection and privacy commissioners from every continent. He also continued to pursue new initiatives, such as the Ethics Advisory Group, through which he intends to stimulate global debate on the ethical dimension of data protection in the digital era.

The EDPS aims to make data protection as simple and effective as possible for all involved. This requires ensuring that EU policy both reflects the realities of data protection in the digital era and encourages compliance through accountability.[66]

## 3. PERSONAL DATA PROTECTION OF THE REPUBLIC OF NORTH OF MACEDONIA

**The first Law on the Protection of Personal Data was adopted in 1994 to regulate the collection, processing and retention of information. This Law defined, organizational and technical measures against the illegal collection, analysis, destruction and disclosure of personal data as well as illegal access to data or databases. In January 2002 this Law was amended, in order to enable an appropriate level of personal data protection, incorporating the principles of the legal processing of personal data, particularly special categories of personal data as established by Directive 95/46/EC. However, implementation of this Law appears to have been sporadic, and the mandated supervisory body for enforcement of the Law was not actually established.**

The harmonization of the legislation of Macedonia in the area of personal data protection and the establishment of an independent regulatory body became a Government priority activity from 2002. Within the context of approximation of the legislation of Macedonia to Directive 95,46/EC, particularly Article 28 stating that " each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by Member State pursuant to this Directive", a new Law on Personal Data Protection was drafted in 2004, amended to include the EC recommendations and eventually adopted on 25th January 2005.

The Parliament of the Republic of North Macedonia adopted the new Law in early 2020.[67] The Law is almost entirely aligned with the GDPR, even though the Republic of North Macedonia is not an EU Member State. Derogations from the GDPR include a lower threshold for the exemption from keeping records of processing activities, special requirements for data protection officers, including the requirement of fluency in Macedonian, and the stipulation that processing for direct marketing purposes can only be conducted based on the data subject's consent. Furthermore, the Law has transformed the Directorate for Personal Data Protection into the Directorate for Personal Data Protection (DZLP), which has been given enhanced powers to, among other things, authorize

66 See Annual Report 2016: https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf.
67 Official Gazette of the RNM, No. 42, 15.02.2020.

standard contractual clauses ('SCCs')[68] and Binding Corporate Rules ('BCRs').[69]

The main purpose of the Law, among others, is the harmonization of the local legislation with EU legislation, i.e. Regulation.[70] Pursuant to the Law, new standards related to the processing of personal data have been introduced. The Law is based on the following principles of personal data processing: (i) lawfulness, fairness and transparency; (ii) limitation of the purposes of personal data processing; (iii) minimum volume of data; (iv) data accuracy; (v) limitation of the retention period; (vi) integrity and confidentiality; and (vii) accountability.[71] Moreover, data controllers and processors are granted with a transition period of eighteen months to align their activities with the Law. The relevant subordinate legislation shall be adopted by the Agency for Personal Data Protection in August 2021. In the meantime, the current subordinate legislation shall remain applicable unless it is in direct conflict with the Law.

The Law includes specific provisions regarding the rights of data subjects to seek administrative and judicial remedy against violations of their rights related to data protection. In case of a violation of the individual's rights under the Law, the individual will be entitled to directly seek remedy before the court against data controllers and processors.[72] The Law provides for penalties ranging between 2%-4% of the total annual income of the legal entity - data controller or processor (in absolute terms), generated in the business year preceding the year when the infringement was committed or of the total income generated for a shorter period than the year preceding the infringement, if the legal entity started conducting business activities in that year.

Macedonia's obligation to align its national legislation with the EU regulatory framework derives from its status as an EU candidate country, whereby the implementation of the EU legislation is mandatory. The Constitution of the North Macedonia guarantees the right to privacy of individuals.[73] There are data protection provisions in many sartorial legislation such as: Law on Criminal Procedure,[74] Low for Health Protection,[75] Law on Electronic Communications[76] etc.

The 'DZLP, is the national regulatory authority that oversees the implementation of the Law.[77]

The Law applies to all organizations (both public and private) in North Macedonia that process the personal data of individuals residing in North Macedonia. The Law also applies to foreign organizations if they:

68 The European Commission can decide that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally. It has so far issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area (EEA). See decision 2001/497/EC and decision 2004/915/EC . It has also issued one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA.. See Decision 2010/87 EU.

69 Binding corporate rules (BCR) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group. The authority will approve the BCRs in accordance with the consistency mechanism set out in Article 63 of the GDPR. See Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01); Recommendation on the approval of the Controller Binding Corporate Rules form (wp264); Recommendation on the approval of the Processor Binding Corporate Rules form (wp265); Working Document on Binding Corporate Rules for Controllers (wp256rev.01); Working Document on Binding Corporate Rules for Processors (wp257rev.01)

70 (EU) 679/2016 of 27 April 2016, commonly known as the General Data Protection Regulation or 'GDPR', as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) of the Council of Europe.

71 Article 10.

72 Articles 97-101.

73 Article 18 of the Constitution: "The security and confidentiality of personal information are guaranteed. Citizens are guaranteed protection from any violation of their personal integrity deriving from the registration of personal information trough data processing. Also, The country is also a signatory to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 108/81.

74 Articles 139-142.

75 Articles 153,167,226a.

76 Articles 49-58.

77 The DZLP has not yet issued guidelines for the implementation of the Law since the Law entered into force on February 2020, but the following documents has been issued: DZLP launches investigation into legality of processing by ministries following failure to notify hacker attack, 13 August 2020; DZLP adopts rulebooks on video surveillance, 15 May 2020; DZLP adopts blacklist and white list on DPIAs, 15 May 2020; DZLP adopts rulebook on data breach notification, 15 May, 2020; DZLP adopts rulebooks on video surveillance, 15, May, 2020; DZLP adopts rulebook on high risk personal data processing, 15 May, 2020; DZLP adopts rulebook on data transfers, 14 May, 2020; DZLP adopts rulebook on security of personal data processing, 02 April 2020; Agency submits annual report 2019 to National Assembly, 18 March 2020; and DZLP announces new Law on Personal Data Protection, 18 February 2020.

- offer goods or services to individuals in North Macedonia; or
- monitor the behaviour of individuals in North Macedonia.[78]

The Law does not apply to the processing of:

- personal data collected by individuals for purely domestic or household activities, with no connection to a professional or commercial activity; and
- personal data collected by competent authorities for the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[79]

The DZLP's main competencies include:

- to promote awareness of the risks, rules, safeguards, and rights pertaining to personal data (especially concerning children);
- to advise national and governmental institutions on the application of the Law;
- to hear claims brought by data subjects or their representatives, and inform data subjects of the outcome of such claims;
- to establish requirements for data protection impact assessments ('DPIAs');
- to encourage the creation of Codes of Conduct and review certifications;
- to authorize Standard Contractual Clauses ('SCC') and Binding Corporate Rules ('BCRs');
- to keep records of sanctions and enforcement actions; and
- to fulfil 'any other tasks related to the protection of personal data.'[80]

## 3.1. Key Definitions and Basic Concepts

**Personal data:** Any information pertaining to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. Common examples of personal data are names of individuals, addresses, telephone numbers, identity card numbers, dates of birth, personal identification number, occupations, account information, and financial information.

**Data controller:** Any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. When a law or regulation determines the purposes and methods of personal data processing, the same law determines the controller or the particular criteria for its selection.

**Data processor:** Any natural person, legal entity, or authorized state administrative body, which process the personal data on behalf of the controller.

**Personal data processing:** Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

78 Article 3 para. 3.
79 Article 2 para. 2.
80 See Articles 65-75 and Articles 57-60, and Articles 64-67.

**Collection of personal data:** Any structured set of personal data which is accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis.

**Data subject:** Any natural person to whom personal data is processed.

**Consent:** Any freely given, specific, informed, and unambiguous indication of his or her wishes by which the data subject, either by a statement or by explicit affirmative action, signifies agreement to personal data relating to them being processed.

**Special Categories of Personal Data:** Personal data that reveals racial or ethnic origins, political, religious, philosophical or other beliefs, membership of trade union organizations, and data relating to human health such as genetic or biometric data, or data which refers to the sexual identity of the individual.

**Data breach**: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

**Data concerning health**: Personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status.[81]

## 3.2. Notification/ Registration

Personal data processing may be performed:

- where the data subject has given consent to the processing of his or her personal data for one or more specific purposes; or
- where such processing is necessary:
  - for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject before entering into a contract;
  - for compliance with a legal obligation to which the controller is subject;
  - to protect the vital interests of the data subject or another natural person;
  - for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller; or
  - for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[82]

The personal identification number of the personal data subject may only be processed:

- where the data subject has given consent to the processing for one or more specific purpose;
- to fulfil the rights and obligations of the data subject or the controller; and
- in other cases as determined by the Law.[83]

The following personal data can be processed only based on prior approval from the DZLP:

[81] See Article 4.
[82] Articles 10-12.
[83] Articles 13-15.

- data concerning the health of the data subject;
- genetic data, except if the processing is for purposes of diagnosis and medical treatment of the data subject; and
- biometric data.[84]

## 3.3. Data Controller and Data Processor Rights and Responsibilities

The data controller must inform the data subjects of the data processor who will process their personal data, the legal purposes for the processing of their personal data, and the type of processing activities which are to be applied to their data. Such information must be provided in a concise, transparent, intelligible, and easily accessible form, using clear and understandable language. Any information provided to children should be in a clear and understandable language such that a child can easily understand it.[85]

The data controller also must ensure that the collected personal data is relevant and necessary for the legal purposes for which it is collected, and to ensure, on an ongoing basis, that the data is accurate, complete, and updated. The data controllers' responsibilities also include:

- to implement appropriate technical and organizational measures to ensure and to keep records of their processing activities to demonstrate that they are compliant with the requirements of the Law;
- to implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure, or access;
- to ensure that, both in the planning phase of processing activities and the implementation phase of any new product or service, the data protection principles, and appropriate safeguards, are addressed and implemented (i.e. Privacy by Design);
- where two or more data controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers who must, through an 'arrangement' **between** them, apportion data protection compliance responsibilities;
- a data controller established outside North Macedonia must appoint a representative if the data controller offers goods or services or monitors individuals in North Macedonia unless the processing is occasional, small-scale, and does not involve sensitive personal data; and
- a data controller that wishes to appoint a data processor must only use data processors that guarantee compliance with the Law.[86]

Like with the data controller, the data processor must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure, or access. Depending on the nature of the processing, such measures may include:

- encryption of the personal data;
- security testing; and
- periodical review of security measures and others.[87]

[84] Article 13 (8,9).
[85] Article 16 (1).
[86] Article 17. Also, see Articles 28-35.
[87] Article 36.

The data controller and the data processor are jointly responsible for ensuring compliance with the Law and for any potential infringements. Data processors have statutory obligations in their own right under the Law.

Individuals and the DZLP can hold both data controllers and data processors to account if they fail to comply with their responsibilities under the Law. However, a data processor is liable for the damage caused by its processing activities only where it has:

- not complied with obligations under the Law that are specifically directed to processors; or
- acted outside or contrary to the lawful instructions of the data controller.

A data controller and a data processor must enter into a binding written agreement to manage their relationship. Under the agreement the processor must:

- only act on the data controller's documented instructions;
- impose confidentiality obligations on all personnel who process the relevant data;
- ensure the security of the personal data that it processes;
- abide by the rules regarding the appointment of sub-processors;
- implement measures to assist the data controller in complying with the rights of data subjects;
- support the data controller in obtaining approval from the DZLP where required;
- at the data controller's election, either return or destroy the personal data at the end of the relationship; and
- provide the data controller with all information necessary to demonstrate compliance with the Law.

## 3.4. Data Subject Rights and Data Protections

Under the Law, data subject rights include:

- the right to be informed about the collection and use of their personal data;
- the right of access to their personal data;
- the right to rectification;[88]
- the right to erasure;[89]
- the right to restrict;[90]
- the right to data portability;[91]
- the right to object to the processing of their personal data; and
- rights concerning automated decision making and profiling.

Data subjects are also entitled to receive notice when any inaccurate data concerning them may have been disclosed.

The appointment of a data protection officer ('DPO'), tasked with ensuring data controller compliance with the Law and other applicable regulations, is compulsory only for data controllers and data processors whose core activities:

88 That is, to have inaccurate personal data rectified, or completed if it is incomplete.
89 That is, to have their personal data erased.
90 That is, to request the restriction or suppression of the processing of their personal data.
91 That is, to move, copy, or transfer personal data from one data controller to another safely and securely, without affecting its usability.

- require large scale, regular, and systematic monitoring of individuals (for example, online behaviour tracking); or
- consist of large-scale processing of special categories of data or data relating to criminal convictions and offences.[92]

DPOs must:

- inform and advise the highest level of management and employees about obligations to comply with the Law;
- monitor compliance with the Law, and with data protection policies, including managing internal data protection activities, raising awareness of data protection issues, training staff, and conducting internal audits;
- advise on, and to monitor, DPIAs;
- cooperate with the DZLP; and
- be the first point of contact for the DZLP and for individuals whose data is processed (employees, customers and others).[93]

Finally, high penalties has been introduced in line with the GDPR. The Law prescribes significantly higher penalties for controllers and processors compared to the previous Law on Data Protection. Under the new Law, the fines are set at up to 4 % of the company's total annual income in the preceding financial year.[94]

## 4. GDPR IN THE REPUBLIC OF NORTH MACEDONIA

Some of the most important novelties are set out below:

- Extension of the territorial application of the Law;[95] The application of the Law has also been extended to the processing of personal data of persons from Macedonia by controllers or processors not established in Macedonia, if the processing activities are related to the offer of goods or services to a data subject in Macedonia, whether for payment or not, and to monitoring the activities of the data subject if carried out in Macedonia. In addition, the Law is applied to personal data processing by a controller not established in Macedonia but in a territory where the law of Macedonia is applicable by virtue of international public law.
- Video surveillance;[96]
- Damage compensation and liability;[97]
- Transfer of personal data to third countries and international organizations;[98] Under

92 Article 41.

93 Article 43.

94 Articles 110-112. Under the previously valid Law on Data Protection, the maximum fine was only EUR 2,000.

95 The more precisely defined and extended territorial application of the Law is a significant change, as it applies to the processing of personal data by a controller or processor established in Macedonia, regardless of whether the data processing is carried out in Macedonia or outside its borders.

96 The Law envisages much higher penalties for violations by the controller of the video surveillance provisions, ranging from EUR 1,000 to EUR 10,000. Currently, the maximum penalty for such a violation is EUR 1,000.

97 The Law more precisely defines damage compensation as material and non-material. Crucially, the Law envisages liability for damage compensation not just for the controller, but also for the processor, i.e. the right of the person who suffered damages to sue the controller or processor. Additionally, the Law envisages joint responsibility for controllers or processors allowing for the damaged person to request damage compensation from any controller or processor, thus opening the possibility for the controller or the processor who paid the full damage compensation to request from the other controllers or processors compensation corresponding to their part of the liability for the damage caused. However, this might lead to additional court proceedings.

98 Unlike the previous law, the Law regulates not only the transfer of personal data to third countries, but also to international organizations, including the further transfer from third countries or international organizations to other third countries or international organizations.

the Law, the transfer to a third country or international organization is possible (i) if the Macedonian Agency for personal data protection ("**Agency**"), upon an assessment reaches a decision that the third country or international organization provides an adequate level of protection, (ii) without assessing whether the third country or international organization provides for an adequate level of protection, i.e. if the controller or the processor doing the transfer provides appropriate protection measures (having obligatory corporate rules included in the appropriate measures), and (iii) without reaching a decision on whether the third country or international organization provides an adequate level of protection or the controller or the processor doing the transfer provides appropriate protection measures (having obligatory appropriate measures included in the appropriate measures), but by fulfilling one of the explicitly defined cases in the Law, such as if the data subject has provided explicit consent to the data transfer.

Unlike the previously applicable law, which requires a handwritten form of consent, the Law now includes an extended definition of consent. Consent is now defined as any freely given, specific, informed and unambiguous expression of will of the personal data subject, by which that person, through a statement or clear affirmative act, grants their consent to the processing of personal data relating to them.

For the first time, the consent to processing of the personal data of a child is prescribed. Thus, in relation to directly offering information society services to a child, the processing of the personal data of a child will be lawful where the child is at least 14 years old. If the child is below 14, it is lawful only if the consent is given or allowed by the child's legal representative.

The controller is obliged to notify the data subject of the breach without delay if the breach can result in a high risk to the data subject's rights and freedoms. The controller is obliged at the data subject's request to provide a copy of the data being processed free of charge. The delivery may also be made electronically. This change significantly increases transparency and improves the position of data subjects.

Right to correction of data: This right allows incorrect data about the data subject to be corrected, without undue delay. In addition, the data subject has the right to supplement incomplete personal data by providing an additional statement. The data subject is entitled to ask the controller to erase personal data, to cease further data transmission, and to stop the processing of data by third parties in the case of erasure of data.

Data must be erased if it is no longer necessary to achieve the purpose of the processing or if consent to processing has been revoked. When deciding on a request for data erasure, it is also necessary to consider the public interest in the availability of these data, which may outweigh the private interest in erasing it, in which case there will be no erasure (the Law prescribes other exceptions from this rule).

Also, The data subject is entitled to limit the processing of their data by the controller in the following cases: (i) if the data subject contests the accuracy of the data; (ii) if the processing is illegal, and the data subject is opposed to erasure and instead requests restriction of the use of the data; (iii) if the controller no longer needs the personal data for the purpose of the processing, but the data subject requested it for the purpose of submitting, exercising or defending a legal claim; and (iv) if the data subject has lodged an objection to the processing, and the assessment of whether the legal basis for processing by the controller prevails over the interests of that person is ongoing.

The person that previously provided data to the controller will have the right to receive the data from the controller in a structured, commonly used and machine-readable format, and the right to transmit this information to another controller, without interference from the first controller.

More precise and detailed definition of personal data. The Law introduces a more precise and detailed definition of personal data to ensure the broadest legal protection possible for individuals. Personal data is thus defined as any data that refers to a natural person whose identity has been determined or is determinable, directly or indirectly, based on identity parameters, such as name or identification number, location data, identifiers in electronic communication networks or one or more features of the person's physical, physiological, genetic, mental, economic, cultural or social identity. According to the Law, a natural person can now be determined based on identifiers in electronic communication networks, based on their devices, applications, tools and protocols, such as internet address protocols, cookie identifiers or other identifiers, such as radio frequency labels.

Protection measures: The controller will be obliged to implement necessary protection mechanisms during processing to protect the rights and freedoms of data subjects. When determining the processing method, or during processing, the controller will be obliged to (i) use appropriate technical and organizational measures, such as pseudonymmmisation, aimed at ensuring the effective application of personal data protection principles, such as reducing the amount of data; and (ii) ensure the application of necessary protection mechanisms during processing to meet conditions for processing as prescribed by the Law and to protect the rights of data subjects.

The controller is obliged to ensure through the application of technical and organizational measures that only those personal data necessary for the realization of each individual processing purpose are processed in an integrated manner. This refers to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. These measures need to ensure that the personal data, without the consent of the data subjects, are not automatically available to an unlimited number of natural persons.

Legal remedies and liability: The Law abandons the right to appeal as a legal remedy and prescribes the right to directly initiate an administrative dispute against the decisions rendered by the Agency. Another legal remedy available to the data subject is an objection to the controller on the manner in which their personal data are processed. Several personal data protection measures (technical and organizational) are prescribed:

- pseudonymisation and cryptographic data protection;
- ensuring indefinite confidentiality, integrity, availability and resilience of processing systems and services;
- re-access and availability in case of physical or technical disruption; and
- regular testing, assessment and evaluation of processing safety measures.

Not later than 72 hours after having become aware of a personal data breach, the controller is obliged to notify the Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Privacy impact assessment (PIA): If some type of processing is likely to result in a high risk to the rights and freedoms of natural persons, in particular due to the use of new technologies and taking into account the nature, scope, circumstances and purpose of processing, before starting the processing the controller will assess its impact on personal data protection. The Law further specifies cases in which an impact assessment is required. These include large-scale systematic surveillance in public areas, and systematic and comprehensive assessment of the status and characteristics of a natural person with the aid of automated processing, including profiling, etc.

Under the previously adopted law on personal data protection, the controller does not have an

obligation to appoint a Data Protection Officer (DPO) if (i) it does not have more than 10 employees, or (ii) the processing refers to the personal data of members of associations founded for political, philosophical, religious or trade-union purposes.

The Law provides that the DPO will have to be appointed when the core activities of the controller or processor consist of processing operations which, by their nature, scope or purpose, require regular and systematic monitoring of many data subjects or processing of special categories of data or processing of personal data related to criminal convictions and criminal acts specified in the Law.

## Conclusion

Article 16 of the Treaty on the Functioning of the European Union (TFEU) conferred very broad competences to the Union to legislate on data protection matters. On the basis of this provision, it would have been possible to establish a uniform data protection regime applicable to all processing operations of personal data falling within the scope of EU law. However, one size does not fit all, and the co-legislators, therefore, opted for a separate legal instrument, the Directive for police and criminal justice authorities. The LED adopts some of the GDPR's solutions, but also has many standalone, distinct features. The Directive is undoubtedly a major step forward[99] compared to the data protection rules the EU had established under its third pillar (Justice and Home Affairs) prior to the entry into force of the Lisbon Treaty.

The Directive contains a comprehensive and forward-looking set of rules, receptive towards law enforcement activities in the Digital Age. This was demonstrated on the examples of principles (purpose limitation and data minimization) that are more flexible than the equivalent provisions under the GDPR. The same holds true for some of the novel features introduced by the Directive, such as the use of logs for criminal proceedings, the possibility for competent authorities to carry out a self-assessment of appropriate safeguards surrounding international transfers, or the derogation allowing international transfers directly to private parties in third countries. At the same time, the LED empowers data subjects with a strong set of rights and offers a higher level of protection. Moreover, the mechanism for independent oversight by competent authorities through the supervisory authorities and the indirect exercise of data subject rights were illustrated and the detailed rules on the obligation for competent authorities to keep logs of the processing activities in law enforcement databases, as one of many new obligations of the competent authorities under the Directive were explained.

The Directive shows that it now will be possible to achieve high privacy and data protection standards while processing personal data for law enforcement purposes in a more flexible manner. It would, therefore, be instrumental to shift the public debate from the false paradigm that either one or the other may be achieved. Today, the LED presents a benchmark for the consolidation and alignment of other EU data protection rules in the area of police cooperation and judicial cooperation with its rules (Article 62(6)).[100]

Despite all, the effectiveness of the Directive will largely depend on its transposition within the

[99] See Paul de Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive', p. 17 and Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33 (2017), 324-340.

[100] By May 2019, the Commission has to propose the alignment of regimes such as Prüm (Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 1–11 and Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, p. 12– 72, or the Swedish Initiative (Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100). Moreover, the rules of the Directive have been taken over for some EU agencies active in this area. See in particular the Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p. 1–71.

legal system of each individual Member State. The general applicability of the Directive and the wide discretion of national legislators as to achieving the instrument's objectives might lead to considerable variations among the Member States, as was the case with the implementation of, for instance, Article 15 of the DPD. In particular, there are risks of an overly broad interpretation of the scope of the Directive, at the expense of the GDPR. This situation is generated by the ambiguous language of Article 1(1) of the Directive and its accompanying Recital 12. They seem to broaden the applicability of the Directive from the core criminal law enforcement realm to the 'safeguarding against and the prevention of threats to public security' when certain police actions, such as undertaken during the major sporting events, riots or demonstrations may or may not lead to a criminal offence. Moreover, despite Recital 13 of the Directive, the latter left the notion of 'criminal offence' completely undefined, thereby making it entirely dependent on the interpretation of that notion under national law.

The powers of supervisory authorities are yet another area where the transposition might turn out to be fragile, while the full potential of the Directive can be achieved only through a strong enforcement of its rules by these authorities. This is another weakness of the Directive, concretely its Article 47. Unlike the GDPR, which is very explicit on the powers of the supervisory authorities in its Article 58, the Directive does not oblige the Member States to vest their national supervisory authorities with any particular corrective powers in respect of police and criminal justice authorities, rather providing a few examples under Article 47(2) and introducing a general requirement that such powers need to be effective. In any event, there are no valid reasons to undermine the full transposition of the Directive, given that 'the police should follow what is in the Directive anyway'.[101]

One of the key novelties in the North Macedonia Law is the wider scope of the application of the Law, with an obligation for the locally based controllers and processors to apply the Law regardless of whether the data processing happens within or outside the borders of North Macedonia. More importantly, foreign entities also must follow the local requirements if the data processing covers the offering of goods or services (even free of charge) to or monitoring the behaviour of individuals from North Macedonia.

The law applies to any form of automated data processing done in North Macedonia, regardless of if the data originated from North Macedonia or another country. Standards and principles for data processing, lawful bases and data subject rights are also included in the legislation.

"… penalized for breach of privacy policy …. facing a complaint regarding personal data protection …"[102]

GDRR has raised awareness of the concept of privacy and the draconian fines have encouraged the companies to pursue a new level of security in the use and processing of users' personal data.

GDPR has raised awareness in relation to the concept of privacy, and the draconic sanctions have pressured the companies to strive to achieve a new level of security in using and processing personal data.

In February 2020, the Republic of North Macedonia adopted the new Law on Personal Data Protection, in order to harmonize the existing legal framework in the field of protection of personal data with the GDPR standards.

The law prescribes a time period of 18 months in which the controllers and processors are obliged to comply their work with the provisions of the new law, that is, up to 24 August 2021.

LPDP imposes a more active role of the controller who will have to undertake measures for

[101] Valsamis Mitsilegas, scholar of European Criminal Law at Queen Mary University of London, during the House of Lords EU Committee session on Brexit and EU data protection, 17 July 2017.

[102] These are just some of the headlines that were and are current after the Regulation (EU) 2016/679 – General Data Protection Regulation became enforceable in May 2018 (GDPR).

improvement, upgrade and adjustment of its established system for personal data protection, i.e. each controller will have to perform in-depth analysis and assessment to determine the level of compliance of the existing system with the new legal solution. The controller and the processor are also obliged to apply appropriate technical and organizational measures to ensure and be able to prove that the processing of personal data is carried out in accordance with the provisions of the law.

The Personal Data Protection Agency on its official website has published information for the controllers in regards to the application of the new law, related to the activities for improvement, enhancement and adjustment with the established systems for data protection.

As a way to raise the level of personal data protection, the law also recommends the adoption of Code of Conduct and Certification[103] that would be applied in the operations of controllers and processors.

LPDP envisages supervision regarding the application of the law, and depending on the severity of the misdemeanor, imposes fines in the amount of up to 2% -4% of the total annual income of the controller or processor-legal entity, (expressed in absolute amount) realized in the business year preceding the year when the misdemeanor was committed or of the total income earned for a shorter period of the year preceding the misdemeanor, if in that year the legal entity has started working, as well as fines in the amount of 300 to 500 euros in Macedonian denars for the responsible person at the legal entity.[104]

Therefore, taking into account that the new law provides many amendments and new activities for the controllers and the processors, as well as that the subjects of personal data gain more rights, the companies must use the legally provided period of 18 months reasonably in order to harmonize their work with the new regulations.

The Law harmonises with the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and sets out, among other things, principles related to data processing, lawful bases, and data subject rights., even though North Macedonia is not an EU Member State. The Law applies to wholly or partially automated personal data processing, and addresses controller or processor establishment in the territory of the Republic of North Macedonia, as well as whether the data is processed on the territory of the Republic of North Macedonia or beyond its borders. Also, the Law is almost entirely aligned with the GDPR, but derogations are mainly introduced in terms of procedure and for certain specific data processing situations. The following derogations and special rules under the Law are to be noted:

- lower threshold for the exemption from keeping records of processing activities;
- special requirements for data protection officers, including fluency in Macedonian;
- the requirements for personal data transfers envisaged in the Law do not apply to transfers from North Macedonia to countries within the EU/EEA, which are subject only to notification before the Agency for Personal Data Protection ('the Agency'). Transfers to third countries, on the other hand, should comply with the transfer requirements set out in the Law (similar to the relevant provisions of the GDPR) and also require the prior approval of the Agency;

[103] The Code of Conduct, see Definition of Code of Conduct (bizfluent.com).

[104] A number of other changes concern the data protection authority, which is now an Agency for Personal Data Protection, the Central Registry of Personal Data Collections, the cross-border processing, the notifying obligations, etc. From this perspective, 24 August 2021 as the end date for harmonization of the processing activities might seem far away; however, all-around measures can arise only from proper and well-timed assessments. Hence, the sooner the companies start with the necessary preparations the better. During the same period, the Agency will be quite busy with adapting its activities and enacting the necessary secondary legislation.

- unless explicitly required by law, the processing of health, genetic and biometric data requires the prior approval of the Agency, even if it is based on the data subjects' consent; and
- processing for direct marketing purposes can only be conducted based on the data subject's consent.

Article 10 of the Law contains the legal basis for the lawful processing of data. These are data subject's consent, the fulfilment of a contract to which the data subject is party to, legal obligations of the controller, the protection of the vital interests of the data subject or another person, public interest or the performance of a public function as established by law. The Law also provides the controller's legitimate interest or the legitimate interest of a third party as a lawful ground for processing, except where such interest overrides the interests or the underlying rights and freedoms of data subjects, especially when the data subject is a child.

In addition, Article 11 of the Law sets out the terms of consent. If consent is given in writing, the request for consent must be presented in a way that can be clearly distinguished from other terms, and it must be comprehensible and easy to understand. In case of a child under the age of 14, processing is legal only if consent is given by the child's legal representative.

Under the Law, the existing data protection regulatory authority, DZLP, is transformed into the Agency. The Agency is empowered with much broader competencies than its predecessor to oversee the enforcement of the Law, investigate breaches of the Law, and bring legal proceedings where necessary. [The Agency's mandate] includes to:

- promote awareness of the risks, rules, safeguards and rights pertaining to personal data (especially in relation to children);
- advise national and governmental institutions on the application of the Law;
- hear claims brought by data subjects or their representatives, and inform data subjects of the outcome of such claims;
- establish requirements for Data Protection Impact Assessments ('DPIA');
- encourage the creation of codes of conduct and review certifications;
- authorise model clauses and Binding Corporate Rules;
- keep records of sanctions and enforcement actions; and fulfil any other tasks related to the protection of personal data.

Moreover, if the DPIA shows that the processing will cause a high risk to data subjects, controllers must consult the Agency prior to the processing. Furthermore, in case of a personal data breach, the controller must notify the Agency immediately and not later than 72 hours after learning about it, unless it is likely that the breach will not result in a risk to the rights and freedoms of individuals. The Agency is empowered to impose administrative fines to a controller or processor in breach of the rules of up to 4% of the annual worldwide turnover of the preceding financial year. Additionally, an individual who has suffered harm as a result of the unlawful processing of their personal data has the right to receive compensation from the controller or processor for the harm suffered.

Finally, compliance with the Law will be a complex and time-consuming process, which will require the involvement of different stakeholders within the company. Practical measures should be taken, such as adopting the required internal documentation and putting in place appropriate technical and

organizational measures. Taking into account that compliance with the new legal framework cannot be achieved overnight, Parliament has envisaged a transitional period of 18 months for companies to align their operations with the new requirements. Thus, the Law has largely adopted provisions and solutions from the GDPR, it remains to be seen whether its effective implementation will be achieved or if North Macedonia will remain behind EU countries with respect to fundamental rights to privacy and personal data protection.

# List of References


1. A handbook of European Data Protection Law, Luxemburg, Publications Office of the European Union, 2018.
2. Andrew Guthrie Ferguson 'The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement', NY: New York University Press, 2017.
3. Annual Report 2016: https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_en_1.pdf.
4. Bărbulescu v. Romania [GC], §§ 108-111 as to the actions of a private employer.
5. Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics', in: Philos. Technol. 2017, 30: 475.
6. Case C 101/01.
7. Case C-342/12.
8. Case C-465/00. C-138/00.
9. Case C-468/10 and C-469/10.
10. Case C-92/09 and C-93/09.
11. Case Law Overview 1 December 2014 - 31 December 2015, Working Document, Relevant case-law of CJEU, ECHR and national courts of EU Member States on the right to the protection of personal data, the right to the protection of private life, access to documents and the right to freedom of expression. Includes reference to pending cases. European Data Protection Supervisor 15 March 2016.
12. Case T-164/09 and T-237/16.
13. Case C-524/06.
14. Case C-553/07.
15. Christine Goodwin v. the United Kingdom [GC], § 90. v. the United Kingdom, § 71).
16. CJEU C-362/14, Maximilian Schrems, ECLI:EU:C:2015:650.
17. Convention 108, ETS No.108.
18. Council Decision 2008/615/JHA of 23 June 2008 on the offices and agencies and on the free movement of such data.
19. Council Decision 2008/615/JHA of 23 June 2008.
20. Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA.
21. Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016.
22. Council Framework Decision 2008/977/JHA.
23. Council of Europe, Guidelines to respect, protect and fulfill the rights of the child in the digital environment, 2018.
24. Council of Europe, Automated medical data banks ,1981.
25. Council of Europe, Communication to third parties of personal data held by public bodies, 1991.
26. Council of Europe, Convention on Protection of health-related data, 2019.
27. Council of Europe, Data used for employment purposes, 1989.
28. Council of Europe, Direct marketing, 1985.
29. Council of Europe ,Guide to human rights for Internet users, 2014.

30. Council of Europe Medical and genetic data ,1997.
31. Council of Europe, On the protection of personal data collected and processed for insurance purposes, 2002.
32. Council of Europe, Personal data collected and processed for statistical purposes,1997.
33. Council of Europe, Personal data in the area of telecommunication services, telephone in particular, 1995.
34. Council of Europe, Police files, 1987.
35. Council of Europe Privacy on the Internet,1999.
36. Council of Europe, Profiling , 2010.
37. Council of Europe, Protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, 2016.
38. Council of Europe, Protection of human rights with regard to social networking services, 2013.
39. Council of Europe ,Scientific research and analysis, 1983.
40. Council of Europe ,Social security, 1986.
41. Council of Europe, The processing of personal data in the context of employment, 2015.
42. Council of Europe, The processing of personal health-related data for insurance purposes, including data resulting from genetic tests, 2016.
43. Council of Europe, The roles and responsibilities of internet intermediaries, 2018.
44. Council Regulation (EU) 2017/1939 of 12 October 2017.
45. Caase C-139/01.
46. Decision 2004/915/EC.
47. Decision 2008/615/JHA.
48. Decision No 1247/2002/EC, OJ L 295, 21.11.2018.
49. Definition of Code of Conduct (bizfluent.com).
50. Diana Alonso Blas, First pillar and third pillar: need for a common approach on data protection? In: Gutwirth, S., 'Reinventing Data Protection?', Springer, Berlin (2009).
51. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.
52. Directive 95/45/EC.
53. ECtHR App no 37138/14 Szabò and Vissy v. Hungary (12 January 2016).
54. ECtHR App no 47143/06 Roman Zakharov v. Russia (11 December 2015).
55. ECtHR App nos 30562/04 and 30566/04 S and Marper v United Kingdom (4 December 2008)2008] .
56. EU Directive 2016/680.
57. European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017.
58. Evans v. the United Kingdom [GC], § 75.
59. Evans v. the United Kingdom [GC], § 77; v. the United Kingdom [GC], § 78.
60. FRA et al. (2018).
61. Franziska Boehm 'Information sharing and data protection in the Area of Freedom, Security and Justice – Towards harmonized data protection principles for EU-internal information exchange', Springer 2012.
62. Fretté v. France, § 42; Odièvre v. France [GC], §§ 44-49.
63. From Individual to Group Privacy in Big Data Analytics | SpringerLink.

64. Gaskin v. the United Kingdom, § 42.
65. Hämäläinen v. Finland [GC], § 65.
66. Hämäläinen v. Finland [GC], § 66; X and Y v. the Netherlands, §§ 24 and 27.
67. Kroon and Others v. the Netherlands, § 31.
68. Kuner, Christopher, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines (September 15, 2014). Final version published as "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges", in: Burkhard Hess and Cristina M. Mariottini (eds.), Protecting Privacy in Private International and Procedural Law and by Data Protection 19-55 , LSE Legal Studies Working Paper No. 3/2015, Available at SSRN: https://ssrn.com/abstract=2496060 or http://dx.doi.org/10.2139/ssrn.2496060.
69. Case Libert v. France, §§ 40-42.
70. Case Lozovyye v. Russia, § 36.
71. Case Mockutė v. Lithuania, no. 66490/09, 27 February 2018; and • Bărbulescu v. Romania [GC], no. 61496/08, 5 September 2017.
72. Case Nadia Purtova (2017), 'Between GDPR and the Police Directive: Navigating through the maze of information sharing in Public-Private Partnership', available at SSRN: https://ssrn.com/abstract=2930078. Electronic copy available at: https://ssrn.com/abstract=3285873 Cole/Boehm GDPR Commentary (forthcoming Edward Elgar Publishing, 2019).
73. Case Nadia Purtova (2017), 'Between GDPR and the Police Directive: Navigating through the maze of information sharing in Public-Private Partnership', available at SSRN: https://ssrn.com/abstract=2930078.
74. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD, 2013.
75. Official Gazette of the RNM, No. 42, 15.02.2020.
76. Official Journal of European Union, C 326/392, 26.10.2012.
77. OJ L 386, 29.12.2006.
78. OJ L 386, 29.12.2006.
79. OJ L210/1 (6 August 2008).
80. OJ L210/12, 6 August 2008.
81. OJ L386/89, 29 December 2006.
82. Paul de Hert&JurajSajfert, 'The role of the data protection authorities in supervising police and criminal justice authorities processing personal data', in: Briere, C. and Weyembergh, A (eds), The needed balances in EU Criminal law: past, present and future, Hart Publishing, 2017.
83. Paul de Hert and JurajSajfert 'Police, privacy and data protection from a comparative legal perspective" in Monica den Boer (editor), "Comparative policing', Edwar Elgar Publishing, forthcoming in 2018.
84. Paul de Hert and VagelisPapakonstantinou 'Data protection policies in EU Justice and Home Affairs. A multi-layered and yet unexplored territory for legal research', in Ariadna Ripoll Servent& Florian Trauner (eds), Routledge Handbook of Justice and Home Affairs Research, Routledge, London, 2018.
85. Paul de Hert, VagelisPapakonstantinou and Cornelia Riehle 'Data protection in the third pillar: cautious pessimism', in Martin Maik (Editor), Crime, Rights and the EU: The Future of Police and Judicial Cooperation, London, Publisher: Justice, 2008.

86. Prüm (Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008.
87. Recommendation on the approval of the Controller Binding Corporate Rules form (wp264).
88. Regulation (EC) No 45/2001.
89. Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004, OJ L 364, 9.12.2004.
90. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
91. Regulation (EU) 2018/1725 of the European Parliament and of the Council.
92. Roche v. the United Kingdom [GC], § 157.
93. S.H. and Others v. Austria [GC], § 94). SatakunnanMarkkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, 27 June 2017.
94. SatakunnanMarkkinapörssi Oy and Satamedia Oy v. Finland [GC]; (no. 931/13, §§ 133 - 138, 27 June 2017).
95. Series A no. 305-B, opinion of the Commission, 1995.
96. The Council Decision 2008/616/JHA of 23 June 2008.
97. The Council Framework Decision 2006/960/JHA of 18 December 2006.
98. The ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council, OJ L 201, 31.7.2002.
99. The Official Journal of the European Union, 5.6 2015.
100. The Swedish Initiative (Council Framework Decision 2006/960/JHA of 18 December 2006.
101. Thomas Marquenie 'The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework', Computer Law & Security Review, 33, 2017.
102. ValsamisMitsilegas, scholar of European Criminal Law at Queen Mary University of London, during the House of Lords EU Committee session on Brexit and EU data protection, 17 July 2017.
103. Working Document on Binding Corporate Rules for Controllers (wp256rev.01).
104. Working Document on Binding Corporate Rules for Processors (wp257rev.01).
105. Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01).
106. X, Y and Z v. the United Kingdom, § 44; Fretté v. France, § 41.
107. 95/46/EC (General Data Protection Regulation), 27 April 2016.

# METHODOLOGY

The right to object to processing is important although somewhat limited in practice. The main limitations are when the data is processed under some form of official authority or public interest task, normally by the public sector, and when organizations claim a legitimate interest as the basis.

We conducted a qualitative analysis of the awareness and understanding held by North Macedonia organizations. Despite its limitations, we hope this interviews provide insight into public perceptions of data protection rights and help form a baseline to compare future similar analyses once that GDPR has been fully implemented.

Questionnaire design is a multi-step process. In addition, Questionnaires allow collection of both subjective and objective data in a large sample of the study population in order to obtain results that are significant, especially when resources are limited. It is a good tool for the protection of the privacy of the participants. The validity of data and information depends on the honesty of the respondent. The questionnaires can measure both qualitative and quantitative data, but is it more appropriate for quantitative data collection.

We spoke to 13 authorized persons[105] for these interviews. We were particularly looking to attract people that did not consider themselves experts in data protection issues. The interviews lasted 3 days. We informed interviewees of the nature of the research and that we planned to write up what they said for this report.

## 1. Research Themes

We wanted to gain a better view of how authorized persons who are non-experts think about data protection issues. As a top level question, we wanted to see how authorized persons understood data protection law and their data protection rights. We also wanted to see how they thought organizations should behave when collecting and processing data about them.

We wanted to gain a better view of how authorized persons who are non-experts think about data protection issues. As a top level question, we wanted to see how authorized persons understood data protection law and their data protection rights. We also wanted to see how they thought organizations should behave when collecting and processing data about them.

## 2. Research Findings

With General Data Protection Regulation (GDPR) in effect, financial institutions in the EU and beyond must manage their Anti Money Laundering (AML) compliance obligations in a new Data Protection Regime.

The GDPR creates, clarifies, and harmonizes data security legislation across all EU member-states – but also affects organizations from outside territories wishing to do businesses within the bloc.

Practically, GDPR limits the ways in which businesses can collect, use, and store the personal data of their customers and clients – it also creates consequences for institutions with AML obligations.

Since AML efforts require an intense focus on personal data, the restrictions introduced by GDPR may represent a challenge for financial institutions. More specifically, the legal scope of GDPR may

[105] Ministry for the Internal Affairs; Ministry of Justice, Public Prosecutor of North Macedonia; Bar Chamber; Notary Chamber; Chamber of Executor; Forensic Bureau; Financial Police; Chamber of Commerce; Association of Banks; .NBRM; Financial Intelligence Unit; and NLB - The Compliance Officer in the Bank.

clash with the way institutions identify customers during their due diligence procedures and how they manage their risk thereafter.

Article 6 of GDPR requires data controllers to establish a legal basis for collecting and processing personal data – including data required for AML purposes. For institutions with AML obligations, the most relevant justifications provided by Article 6 are:

- Article 6(c) – which allows for the processing of personal data "for compliance with a legal obligation to which the controller is subject" –typically, AML laws or sanctions.
- Article 6(f) – which allows for data processing for "legitimate interests", justifiable on a case-by-case basis.

Comply Advantage justifies its data processing activities under Article 6(f) – since that data is necessary to serve our clients' legitimate interests in delivering AML and sanctions compliance.

One of the most significant aspects of the GDPR is Article 17, which introduces the "right to be forgotten". That right allows data subjects to request the deletion of their personal data under certain circumstances. This rule may be in contention with AML law, which requires data to be held long after a business relationship has ended.

Under GDPR Article 17(3)(b), however, legal requirements take precedence over the right to be forgotten. From an AML perspective, the EU's 4th Anti- Money Laundering Directive (4AMLD) introduced the requirement that both customer due diligence and transaction records be retained for 5 years after the end of the customer relationship. In this context, the right to be forgotten would only be enforceable after this period had ended.

Article 28 of GDPR states that data controllers must appoint data processors, like ComplyAdvantage, who can offer and demonstrate "sufficient guarantees" of GDPR compliance. That being the case, it may be necessary to include GDPR compliance requirements – and the right to audit them – in contracts with third-parties. Similarly, the transmission of data between controllers and third-party processors must also be secure and in compliance with relevant GDPR rules.

As a data processor, Comply Advantage offers clients complete clarity over the protections we put in place to safeguard personal data. Our stringent data security policies enable our clients to remain GDPR compliant, while safely performing every necessary AML check.

Even under the GDPR regime, that need entitles you to store personal information and keep an audit trail of checks and processes. Both AML and data protection laws are constantly evolving and in the wake of new legislation, such as the Fifth Anti-Money Laundering Directive (5AMLD).

The impact of the General Data Protection Regulation, effective 25 May 2018, will be felt for some time to come. One area where GDPR will present a significant ongoing challenge for the financial services industry relates to the personal data collection and processing obligations created under anti-money laundering (AML) regulations. The tension between the AML and privacy requirements is not new, but GDPR's ratcheting up of the data privacy requirements brings it into fresh focus.

On the one hand, AML regulations require the collection, processing and analysis of large volumes of personal data, with the aim of preventing the financial services industry from being exploited as a means of laundering money and committing financial crimes. On the other hand, GDPR not only places restrictions on how, when and why personal data can be collected, processed and used, but also broadens the definition of personal data, bringing all information collected under the AML regulations squarely within the jurisdiction of GDPR.

AML rules require the collection, processing and use of personal data for the following overarching tasks to comply with regulatory obligations:

- Customer due diligence (including enhanced and simplified due diligence);
- Transaction monitoring;
- Behavioural monitoring;
- Internal data sharing (including within a group);
- External data sharing (including with regulators and other financial institutions);
- Data sharing for outsourced arrangements; and
- Cross-border processing of data (especially for the processing of international payments).

The European Union (EU) Fifth AML Directive and further proposed changes to it (termed the "sixth" money laundering directive) are also set to broaden the scope of these requirements by extending coverage to new areas such as virtual and digital currencies.

AMLD5 was followed a few months later in November 2018 by the 6th Anti-Money Laundering Directive (AMLD6), which is primarily also an update of AMLD4, and must be transposed by the EU countries on 3 December 2020 latest.

AMLD5's introduction was expedited by the 2015-2017 proliferation of high-profile terrorist attacks in Europe as well as political scandals like the Panama Papers that followed in the wake of AMLD4.

During this period, European lawmakers were stunned by the new levels of sophistication money laundering had attained, as well as the facilitating part that cryptocurrencies played and could potentially continue to play if this behavior remained unchecked.

Therefore, the European Union's lawmakers decided to iterate on AMLD4, in order to provide more robust protection against virtual asset-facilitated crime and greater transparency during crypto transactions.

AMLD5's legislation bolsters AMLD4 in specific areas:

- It updates and improves the EU's current anti-money laundering (AML) and counter-terrorism funding (CFT) policies
- It closes AML4 loopholes still being exploited by financial criminals
- It brings the European Union bloc's AML/CFT efforts in line with the new FATF Standards as updated in June 2019.

GDPR sets out six data protection principles that apply to the processing of personal data. In brief, these principles stipulate that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
- Accurate and, where necessary, kept up-to-date

- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed

- Processed in a manner that ensures appropriate security of the personal data

However, a risk-based approach to AML compliance has many variations. This gives rise to different levels of personal data collection and use, which don't always sit well with GDPR's six lawful bases approach

Considering the results of the interviews, the following are some of the key challenges that financial firms may face as a result of the process of implementation:

- **Documentation of lawful basis – Documentation of lawful basis –** Firms will need to document the legal basis for processing (including collecting of) personal data for the purposes of complying with AML regulations. This can prove challenging, as these rules tend to be principles-based and require the development of a risk-based approach.

- **Rectification of inaccurate data –** Keeping data up-to-date is also now more important under the GDPR. Historically, firms have not always been good at keeping their customer files up-to-date. Now this will have to be considered not just as an AML regulatory obligation but as a GDPR requirement too, especially where the data is being relied upon to make decisions that impact the customers' ability to access banking or financial services. Additionally, where online or other database-sourced searches are conducted to create an AML risk profile for a customer, firms will have to use reliable and reputable data sources, placing additional burden on the financial services industry and data source providers to establish the reliability of the information used.

- **Data security –** Data security is integral to GDPR compliance, and firms will need to review who has access to customer data required for AML compliance, including all data collected and processed as part of KYC activities and transaction monitoring alerts. Firms will have to scrutinize the use of such data and document the access requirements that employees may need to engage with the data. Personal data should be shared on a need-to-know basis. Firms will also have to identify ways to secure "dormant" personal data that is no longer connected to an existing business relationship but must be retained for a period of at least five years for the purposes of AML regulations.

- **Privacy notice –** Given that data subjects have the right to be informed of the processing and usage of their personal data, firms will have to consider the steps that they need to take to inform their individual customers and the beneficial owners (BOs) of various types of corporate customers of the firm's privacy notice and the legal basis for processing their personal data. The fact that these BOs are sometimes two or three steps removed from the relationship with the corporate customer is a complicating factor that will also need to be considered.

- **Retention –** AML rules and/or internal policies may require personal data to be retained long after the business relationship giving rise to processing has come to an end. This is in direct tension with GDPR, which stipulates that data may not be retained "longer than necessary for the purposes for which the personal data is processed."

- **Outsourcing and secure transmission to third parties –** Firms today are outsourcing a wider range of activities. Firms will need to put in place controls to monitor their vendors' and third parties' ability to be compliant with both AML and GDPR regulations. Firms should consider

incorporating these compliance requirements – and the right to audit them – directly into their third-party contracts.

Concerning the question of harmonization of the national legislative framework of personal data protection throughout money laundering investigations, most of the interviewees consider that national legislation is not fully in line with the 4th EU Directive on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing from 2015 (2015/849 EC). At the same time they emphasized that Measures and activities are being taken at the moment to implement the 5th directive of the European Parliament and Council of 2018 with the preparation of a new law on prevention of money laundering and terrorist financing.

Moreover, taking into account the results of the interviews, trast in the effectiveness of the law was not low. Also, we noticed that most of the organizations still did not feel truly in control of their data despite GDPR.

It seems clear that the awareness of the data protection complaints system is satisfactory to the interviewed people. They appear to suggest however that some work should be done to build up awareness and confidence in the GDPR rights around making complaints.

One of the areas we were interested in exploring in these interviews was how understandable the various GDPR rights for deletion, correction, access and so on. Most of the interviewees expressed high awareness of this issue.

## RECOMMENDATION

Regulated bodies should review areas where GDPR and AML regulations overlap, and do so as a matter of priority. Firms must begin documenting the legal basis for collecting and processing personal data and put in place appropriate privacy notices, and they must further assess whether and how they are addressing the challenges highlighted above appropriately. Over the medium term, the tension between these regulations is set to increase as firms incorporate newer data types and technology into their AML compliance controls. For example, where previously firms have perhaps held a copy of a passport, today they may hold a voice pattern or biometric data. As firms launch projects to use these newer data types and technology, compliance with GDPR should be incorporated into their planning from the very beginning – keeping in mind the considerable penalties GDPR will bring for unlawful use and violation of personal data restrictions.

It is also necessary to increase transparency about who really owns companies and trusts to prevent money laundering and terrorist financing via opaque structures; improve the work of Financial Intelligence Units with better access to information through centralised bank account registers; and tackle terrorist financing risks linked to anonymous use of virtual currencies and of pre-paid instruments. Also, the criteria for assessing high-risk third counties and ensure a common high level of safeguards for financial flows from such countries, should be breaded.

The European Union's impending General Data Protection Regulation (GDPR), applies to every company that offers goods or services to the EU and North Macedonia or monitors the behavior of individuals within the EU and North Macedonia. The aim of the GDPR is to ensure that an individual's personal data is stored with consent, for a specific purpose and for a reasonable duration of time.

The GDPR may require a lot of changes for companies that collect, process or store data on North Macedonian citizens. The organizations must address issues like:

- Privacy and security by design;
- Privacy impact assessments;
- Inventories and data-mapping of personal information across all business systems;
- The appointment of a data protection officer (DPO); and
- Evidence to demonstrate reasonable efforts put forth.

Ensuring GDPR compliance requires a concerted effort across an organization's entire executive team as the data protection officer must work with C-level executives and other senior leadership to properly identify and map out data inventories and processes, perform risk assessments, and conduct gap analyses.

Preparing for a significant security compliance change can be overwhelming. The most efficient way to achieve GDPR compliance is through interdepartmental collaboration and the use of technology solutions that automate and validate business needs such as policy compliance, data security and required reporting. As the deadline looms, most organizations should already have started assessing the business impact, devising a company-wide implementation plan and addressing additional resource needs. Every GDPR implementation plan should include the following six steps:

## 1. Raise awareness enterprise-wide

The first step is to raise awareness of the GDPR at all levels of your organization. Develop recordkeeping and monitor best practices, engage in ongoing training outlining breach scenarios and causes, and create a culture of security across the entire organization. Ensure that employees not only understand the impact of these new regulations, but that they feel comfortable raising alerts, and know who to go to, if there is cause for concern.

## 2. Designate a data protection officer

The GDPR outlines specific organizations that must formally designate a DPO, including public authorities (except for courts) and private organizations where the core activities consist of processing operations that require regular and systematic monitoring of personal information on a large scale or large-scale processing of sensitive data or data relating to criminal convictions or offenses.

## 3. Create a data inventory/register

In order to understand the risks associated with how information is processed, stored and transferred, an organization must fully understand the data it collects and processes. Once a detailed inventory list of data types has been created, each data set should be mapped end-to-end throughout the organization's technology infrastructure to identify all physical and virtual places where data is held. This includes customers, employees, and third-party suppliers or vendors. Distribute these lists to internal departments and stakeholders to ensure that all data types and storage locations have been identified.

## 4. Evaluate risk and perform gap analysis

Next, you will need to take your inventory of data and processes and compare it to the GDPR requirements.. Where are the gaps in compliance? Are there areas at risk of non-compliance in the

future? What are the most immediate needs the company must satisfy in order to move toward GDPR compliance?

## 5. Develop a roadmap

Once you have identified all potential GDPR compliance gaps, your organization should develop a roadmap outlining required changes to processes and systems to conform with GDPR requirements. Some of these changes may result in the tightening of existing controls, while others may require that entirely new controls and processes be developed.

## 6. Monitor and report progress and compliance

The GDPR regulations require "security by design," which mandates that all IT professionals build compliance into the design of future business operations that capture, process or store data. The data protection officer should work with all necessary business and IT teams to ensure that operational systems and data management workflows remain compliant and stay up-to-date with any GDPR announcements or changes.

# Annexes(1)

## SELF-ASSESSMENT QUESTIONNARE: COMPLIENCE WITH THE ANTI MONEY LAUNDERING REGULATIONS AND WITH DATA PROTECTION OBLIGATIONS WHEN PROCESSING PERSONAL DATA

This Questionnaire is aimed at those who have responsibilities for data protection, and should be answered (i.e. by the nominated person who is responsible for data protection in your organization); it will also help managers and administrators understand the full range of data protection issues which are faced whenever personal data are processed. The Questionnaire also seeks to identify weaknesses in compliance procedures.

## A. GENERAL MANAGEMENT

1. To what extent do decision-makers in North Macedonia advocate the harmonization of the national legislative framework with the content of directives of the European Parliament and the Council in the field of personal data protection throughout money laundering investigations?
2. In which of the laws relevant to the subject area you find most shortcomings?
3. Are the definitions of the most important terms in the laws sufficiently clear and comprehensive?
4. Has the Law on Personal Data Protection sufficiently regulated issue of personal data protection throughout a money laundering investigation?
5. How do you assess the cooperation of the competent authorities in the subject area?
6. How do you assess the work of our state bodies in the field of establishing cooperation at the international level? Is this type of cooperation in the Law on Prevention of Money Laundering and Terrorist Financing harmonized with the directives of the European Union bodies?
7. Is the risk management at a satisfactory level?
8. Do you have a Policy on data protection in your organization?
   - If yes, how do you judge the policy?
   - If yes, when was the policy last reviewed?
9. Is the policy adequately resourced, and supported by a management infrastructure that can sustain, monitor and review the Policy and generate reports on its effectiveness?
   - If the answer to the above question is 'Yes', how well do you think the Policy is promoted and supported by management?
10. Is there an identifiable person responsible for data protection within your organization?
    - If the answer to the above question is 'Yes', how is that person is supported by management for data protection matters?

11. Do all individuals who are authorized to process personal data (e.g. staff) receive appropriate training, instruction or guidance on data protection?

    - If the answer to the above question is 'Yes', how do you judge the training given?

12. Are you confident that all individuals (e.g. staff) who process personal data understand their data protection obligations associated with that processing?

    - If there are contracts, associated with the processing of personal data, which allow third parties access to personal data, for example data processors, do these contracts specify data protection requirements?
    - If the answer to the above question is 'Yes', how well do you judge the effectiveness of the monitoring/auditing of contractual controls?

13. Is there a folder of documents, or other documentation, which will help to manage and demonstrate compliance with data protection obligations?

    - If the answer to the above question is 'Yes', what is your view on the quality of the information in the folder or in other documentation?

## B. LAWFULNESS OF PROCESSING

1. Has the full extent of the processing, which is authorized by law and/ or regulations, been identified?

2. Has proof of lawful processing been retained?

## C. TRANSPARENCY OF PROCESSING

1. Are Data Subjects made aware, before they provide personal data, of why personal data is being collected and which organizations will use their data?

2. Are there significant practical or technical difficulties in providing the details identified above?

3. Are there reasons (e.g. in the public interest) for not providing such information?

4. When personal data about Data Subjects are provided by other organizations or individuals, are these Data Subjects made aware of why personal data is collected and which organizations will use the data?

5. Is there a significant technical or practical difficulty in providing the details identified above?

6. Are there reasons (e.g. in the public interest) for not providing such information?

### D. QUALITY OF PERSONAL DATA

1. Is personal data assessed as to whether it is 'adequate, relevant and not excessive' in the context of each particular purpose?
2. Are there significant practical or technical difficulties in meeting these criteria in all circumstances?
3. Are there reasons (e.g. in the public interest) for retaining the personal data since the personal data might become relevant in the future?
4. Is personal data assessed for accuracy and checked whether up to date?
5. Are there significant practical or technical difficulties in carrying out such assessments?
6. Before action is taken against a data subject, is the accuracy of the personal data checked?
7. Are there significant practical or technical difficulties in carrying out such checks?
8. Do formal criteria/procedures for the deletion of personal data exist?
9. Are there significant practical or technical difficulties in deleting personal data?
10. Are there reasons (e.g. in the public interest) for not deleting some or all of the personal data?

## E. SECURITY OF PERSONAL DATA

1. Is there a security policy that covers all aspects of the processing of personal data?
   - If the answer to the above question is 'Yes', how do you judge the security policy?
   - If the answer to the above question is 'Yes', how well is the security policy supported and promoted by management?
2. Do security controls or procedures include measures to ensure the integrity of the personal data and of its processing?
3. How effective do you consider the controls/procedures to be?
4. Do security controls or procedures include measures to permit user identification, authentication and authorization for processing?
5. How effective do you consider the controls/procedures to be for the above question?
6. Do security controls include measures to safeguard operating procedures?
7. How effective do you consider the controls/procedures to be for the above question?
8. Do security controls or procedures include measures to facilitate the use of encryption?

9. Do security controls or procedures include measures to invoke a business continuity/ disaster recovery plan?

10. Are there significant practical or technical difficulties in forming such a plan?

11. Do security controls or procedures include measures to establish adequate audit and monitoring arrangements?

12. How effective do you consider these arrangements to be?

13. Do security controls or procedures include measures to safeguard the physical security of the processing environment?

14. How physically secure do you consider your processing of personal data to be?

15. Are staff trained in the necessary security controls and procedures?

16. If the answer to the above question is 'Yes', how do you judge the training given?

17. When did you last receive training/instruction on IT security requirements?

## F. DATA SUBJECTS' RIGHTS

1. Do procedures allow for Data Subjects to be informed of the nature of the processing of personal data, and to receive confirmation as to whether or not personal data about them is processed?

2. Are there significant practical or technical difficulties in providing such information?

3. Are there reasons (e.g. in the public interest) for not providing such information?

4. Do procedures allow Data Subjects to exercise their right of access to personal data which relate to them?

5. Are there significant practical or technical difficulties in providing such information?

6. Are there reasons (e.g. in the public interest) for not providing such data?

7. Do procedures allow Data Subjects to be informed of the logic underpinning any decision-making processing which significantly impacts on them and to challenge such decisions?

8. Are there significant practical or technical difficulties in providing such information?

9. Are there reasons (e.g. in the public interest) for not providing such data?

10. Do procedures have the capability to correct, block or erase personal data (e.g. . in compliance with requests from Data Subjects and/or from the Data Protection Office or Courts), and to notify Third Parties who have received the Data Subject's personal data?

11. Are there significant practical or technical difficulties in providing such information?

12. Do procedures allow Data Subjects to object to the processing of personal data?
13. Are there reasons (e.g. in the public interest) for not allowing such objections?

## G. NOTIFICATION

1. Has a comprehensive census of the processing of personal data been carried out?
2. When was the census carried out?
3. Do procedures anticipate the need to notify details of the processing to the Data Protection Office?
4. Are there practical or technical difficulties in providing such notification?
5. Are there reasons (e.g. in the public interest) for not providing such a notification?

## H. SYSTEM DESIGN

1. Are data protection considerations taken into account during the development, purchase or acquisition of hardware and software?
2. Are changes to the software or processing environment considered in the context of data protection obligations?

# INTRODUCTION

It has been exactly fifteen months since the Republic of North Macedonia adopted the new Law on Personal Data Protection ("**Law**"), largely in compliance with the GDPR, entering into force only a few days after it was promulgated. Controllers and processors were afforded 18 months in which to align their operations with the new Law. While some have already done so, others have 10 months to comply with the provisions.

Some of the most important novelties are set out below:

## High penalties introduced in line with the GDPR

The Law prescribes significantly higher penalties for controllers and processors compared to the previous Law on Data Protection. Under the new Law, the fines are set at up to 4 % of the company's total annual income in the preceding financial year. Under the previously Law on Data Protection, the maximum fine was only EUR 2,000.

## Extension of the territorial application of the Law

The more precisely defined and extended territorial application of the Law is a significant change, as it applies to the processing of personal data by a controller or processor established in North Macedonia, regardless of whether the data processing is carried out in North Macedonia or outside its borders.

The application of the Law has also been extended to the processing of personal data of persons from North Macedonia by controllers or processors not established in North Macedonia, if the processing activities are related to the offer of goods or services to a data subject in North Macedonia, whether for payment or not, and to monitoring the activities of the data subject if carried out in North Macedonia. In addition, the Law is applied to personal data processing by a controller not established in North Macedonia but in a territory where the law of North Macedonia is applicable by virtue of international public law.

## Video surveillance

The Law envisages much higher penalties for violations by the controller of the video surveillance provisions, ranging from EUR 1,000 to EUR 10,000. Previously, the maximum penalty for such a violation is EUR 1,000.

## Damage compensation and liability

The Law more precisely defines damage compensation as material and non-material. Currently, the Law envisages liability for damage compensation not just for the controller, but also for the processor, i.e. the right of the person who suffered damages to sue the controller or processor. Additionally, the Law envisages joint responsibility (*солидарна одговорност*) for controllers or processors allowing for the damaged person to request damage compensation from any controller or processor, thus

opening the possibility for the controller or the processor who paid the full damage compensation to request from the other controllers or processors compensation corresponding to their part of the liability for the damage caused. However, this might lead to additional court proceedings.

## Transfer of personal data to third countries and international organizations

Unlike the previous law, the Law regulates not only the transfer of personal data to third countries, but also to international organizations, including the further transfer from third countries or international organizations to other third countries or international organizations.

Under the Law, the transfer to a third country or international organization is possible (i) if the Macedonian Agency for personal data protection ("**Agency**"), upon an assessment reaches a decision that the third country or international organization provides an adequate level of protection, (ii) without assessing whether the third country or international organization provides for an adequate level of protection, i.e. if the controller or the processor doing the transfer provides appropriate protection measures (having obligatory corporate rules included in the appropriate measures), and (iii) without reaching a decision on whether the third country or international organization provides an adequate level of protection or the controller or the processor doing the transfer provides appropriate protection measures (having obligatory appropriate measures included in the appropriate measures), but by fulfilling one of the explicitly defined cases in the Law, such as if the data subject has provided explicit consent to the data transfer.

## Consent to processing

Unlike the previously applicable law, which requires a handwritten form of consent, the Law now includes an extended definition of consent. Consent is now defined as any freely given, specific, informed and unambiguous expression of will of the personal data subject, by which that person, through a statement or clear affirmative act (*∂ejcmвue*), grants their consent to the processing of personal data relating to them.

For the first time, the consent to processing of the personal data of a child is prescribed. Thus, in relation to directly offering information society services to a child, the processing of the personal data of a child will be lawful where the child is at least 14 years old. If the child is below 14, it is lawful only if the consent is given or allowed by the child's legal representative.

In this respect, the Law complies with the GDPR as the age limit for the lawfulness of the consent is not below 13.

## Rights of data subjects

### Notification of breach

The controller is obliged to notify the data subject of the breach without delay if the breach can result in a high risk to the data subject's rights and freedoms.

### Right to access

The controller is obliged at the data subject's request to provide a copy of the data being processed free of charge. The delivery may also be made electronically. This change significantly increases transparency and improves the position of data subjects.

### Right to correction of data

This right allows incorrect data about the data subject to be corrected, without undue delay. In

addition, the data subject has the right to supplement incomplete personal data by providing an additional statement.

**Right to erasure of data**

The data subject is entitled to ask the controller to erase personal data, to cease further data transmission, and to stop the processing of data by third parties in the case of erasure of data. Data must be erased if it is no longer necessary to achieve the purpose of the processing or if consent to processing has been revoked. When deciding on a request for data erasure, it is also necessary to consider the public interest in the availability of these data, which may outweigh the private interest in erasing it, in which case there will be no erasure (the Law prescribes other exceptions from this rule).

**Right to limit the scope of processing**

The data subject is entitled to limit the processing of their data by the controller in the following cases: (i) if the data subject contests the accuracy of the data; (ii) if the processing is illegal, and the data subject is opposed to erasure and instead requests restriction of the use of the data; (iii) if the controller no longer needs the personal data for the purpose of the processing, but the data subject requested it for the purpose of submitting, exercising or defending a legal claim; and (iv) if the data subject has lodged an objection to the processing, and the assessment of whether the legal basis for processing by the controller prevails over the interests of that person is ongoing.

**Right to data portability**

The person that previously provided data to the controller will have the right to receive the data from the controller in a structured, commonly used and machine-readable format, and the right to transmit this information to another controller, without interference from the first controller.

**More precise and detailed definition of personal data**

The Law introduces a more precise and detailed definition of personal data to ensure the broadest legal protection possible for individuals. Personal data is thus defined as any data that refers to a natural person whose identity has been determined or is determinable, directly or indirectly, based on identity parameters, such as name or identification number, location data, identifiers in electronic communication networks or one or more features of the person's physical, physiological, genetic, mental, economic, cultural or social identity. According to the Law, a natural person can now be determined based on identifiers in electronic communication networks, based on their devices, applications, tools and protocols, such as internet address protocols, cookie identifiers or other identifiers, such as radio frequency labels.

**Protection measures**

The controller will be obliged to implement necessary protection mechanisms during processing to protect the rights and freedoms of data subjects.

When determining the processing method, or during processing, the controller will be obliged to (i) use appropriate technical and organisational measures, such as pseudonymisation, aimed at ensuring the effective application of personal data protection principles, such as reducing the amount of data; and (ii) ensure the application of necessary protection mechanisms during processing to meet conditions for processing as prescribed by the Law and to protect the rights of data subjects.

The controller is obliged to ensure through the application of technical and organizational measures that only those personal data necessary for the realization of each individual processing purpose are processed in an integrated manner. This refers to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. These measures need

to ensure that the personal data, without the consent of the data subjects, are not automatically available to an unlimited number of natural persons.

**Legal remedies and liability**

The Law abandons the right to appeal as a legal remedy and prescribes the right to directly initiate an administrative dispute against the decisions rendered by the Agency. Another legal remedy available to the data subject is an objection to the controller on the manner in which their personal data are processed.

**More complete regulation of personal data security**

Several personal data protection measures (technical and organizational) are prescribed:

- pseudonymisation and cryptographic data protection;
- ensuring indefinite confidentiality, integrity, availability and resilience of processing systems and services;
- re-access and availability in case of physical or technical disruption; and
- regular testing, assessment and evaluation of processing safety measures.

**Notification of a personal data breach to the Agency**

Not later than 72 hours after having become aware of a personal data breach, the controller is obliged to notify the Agency, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

**Privacy impact assessment (PIA)**

If some type of processing is likely to result in a high risk to the rights and freedoms of natural persons, in particular due to the use of new technologies and taking into account the nature, scope, circumstances and purpose of processing, before starting the processing the controller will assess its impact on personal data protection. The Law further specifies cases in which an impact assessment is required. These include large-scale systematic surveillance in public areas, and systematic and comprehensive assessment of the status and characteristics of a natural person with the aid of automated processing, including profiling, etc.

**Data protection officer (DPO)**

Under the previously adopted law on personal data protection, the controller does not have an obligation to appoint a DPO if (i) it does not have more than 10 employees, or (ii) the processing refers to the personal data of members of associations founded for political, philosophical, religious or trade-union purposes.

The Law provides that the DPO will have to be appointed when the core activities of the controller or processor consist of processing operations which, by their nature, scope or purpose, require regular and systematic monitoring of many data subjects or processing of special categories of data or processing of personal data related to criminal convictions and criminal acts specified in the Law.

The key pillars of GDPR are as follows:

- Individuals privacy is respected, and process and systems uphold this.
- Right for the individual to request all data about them is deleted.

- Right to move the data from one data controller to another.
- Individual has control over their own data and how this data may be used.
- Transparency for data handlers, if a breach occurs then the data protection authority and the individuals affected within 72 hours of breach discovery.
- Severe non-compliance fines for businesses who do not adhere to the Regulation.

This Report summarizes the key findings and recommendations of the focus group discussion conducted with the Central Registry, Financial Intelligence Unit and Data Protection Agency from the North Macedonia. The General Data Protection Regulation (GDPR) and the The **5th** Anti-Money Laundering **Directive** (**AMLD5**) governs all businesses in North Macedonia. This is a European regulation to ensure individuals privacy and rights are protected when information about them has been collected or processed.

## Objective

Focus group discussions (FDG) were undertaken to collecting data, relevant views and taking inputs from specific persons, perception of competent people on a particular topic and identify a solution to a specific problem or issue.

## Methodology

We used a qualitative approach to gain an in-depth understanding of compliance with Anti Money Laundering Regulation (AML) and with General Data Protection Regulation (GDPR) with processing Personal Data. The method aims to obtain data from individuals involved in this process rather than from a statistically representative sample of a broader population.

Four focus group discussions (FDG) were conducted with three stakeholders: Central Registry, Financial Intelligence Unit and Data Protection Agency from the North Macedonia to explore their views, about processing GDPR and AML issues.

## Key findings

The main findings from data generated by the focus group discussions are summarized below. In terms of **who is responsible** for implementation of the Data protection obligations arising from the 5th EU Directive? The answer is that it is Personal Data Protection Agency (PDPA), controllers and processors and all interested parties. PDPA will be the main locomotive that will pull in this process of aligning with GDPR. But locomotive without wagons could never be a train. Hence, all controllers, processors and other stakeholders will have to attach to the locomotive in order to have real personal data protection environment that secures privacy of all data subjects.

**If we ask why?** The simplest answer would be, to be aligned with EU *acquis*. But the true answer is far more complex and logical. Real answer is actually to “acknowledge” the fact that, unlike before, today the processing of personal data is increasingly being carried out in an automated manner, and consequently to establish the protection of personal data and setup a privacy law in connection with the personal data processing in the new era. Additionally, it’s because of the country’s citizens and all data subjects in broader sense that live, work, study or stay in that particular country. Namely, in case of a scandal that is related to personal data breach, in this modern digital world, from data subject’s point of view, there is not much of a difference whether you are coming from EU or non EU

country. On the other hand, if the country wants to achieve adequacy level regarding personal data protection, and hence secure free (less administrative) flow of information that contains personal data, then aligning with, and transposing GDPR is a must.

**To the question of what?** GDPR is so powerful that even a narrow study will show that each and every non EU country from the Balkan Peninsula is preparing, or have prepared already, a law that will transpose it. Republic of North Macedonia is not an exception. That is not on the occasion of GDPR only, but mainly because of the new and enhanced solutions in GDPR such are the new concepts (profiling, pseudonymization, genetic data, biometric data...); Principle of accountability; Right to be forgotten; Privacy by Design and by default; Data Privacy Impact Assessment; Data breach notification; Binding corporate rules…

**Finally the question is how?** After the adoption of the Law, PDPA will harmonize its operations and legislation by: adoption of all by-laws, participation in the harmonization of sect oral legislation, controllers and processors shall be obliged to harmonize their operation with the provisions of this Law within the appropriate period from the day this Law enters into force. Also the Draft Law to Prevent Money Laundering and Terrorism Financing will be in compliance with the 5$^{th}$ EU Directive, especially concerning the Personal Data Pprotection.

## Recommendations

Although the Law has largely adopted provisions and solutions from the GDPR, it remains to be seen whether its effective implementation will be achieved or if Macedonia will remain behind EU countries with respect to fundamental rights to privacy and personal data protection.

The new LDPD applies to all data controllers and processors established in North Macedonia, regardless of whether the data processing is carried out within the country or outside its borders. Foreign controllers and processors could also be subject to the LPDP, if their data processing activities are related to the offering of goods and services to North Macedonian data subjects or to the monitoring of their behavior in the country. Hence, in practice, all businesses targeting their services at the North Macedonian market or that have a corporate presence within the country will be required to abide by the new rules.

The state body responsible for monitoring and control of the LPDP is the North Macedonian Data Protection Agency.

In certain aspects North Macedonia has adopted a more stringent approach than the EU regulation and has introduced increased requirements for lawful data processing. These include:

**Additional Consent Requirements**

Under the LPDP, the processing of an individual's personal identification number ("PIN") can only be based on his/her explicit consent, unless the processing of this personal data category is explicitly required by law. If the processing of PINs will be systematic and at a large scale, the data controller must also request the prior approval of the Agency. LPDP further stipulates that processing for direct marketing purposes requires the data subject's consent in all cases

**Approval by the Agency**

The LPDP sets an obligation for data controllers to request the approval of the Agency for processing carried out for the purpose of serving public interest, including processing in relation to social protection and public health. This requirement is valid regardless of any prior consultations conducted with regulatory authorities. The prior approval of the Agency is also required for the processing of health, genetic and biometric data, even when it is based on consent, unless otherwise provided

by law. Another data processing activity where the Agency's approval is required, is personal data transfers outside of North Macedonia to non-EU/EEA countries. The approval by the Agency should be obtained in addition to the application of one of the respective legal grounds for transfers as per the GDPR.

**Requirements to notify the Agency**

Transfers of personal data to countries within the EU/EEA are subject to prior notification of the Agency. The scope and form of such notification are still unclear. Data controllers are further obliged to notify the Agency if the processing of personal data is likely to pose a high risk to the rights and freedoms of individuals (taking into account the nature, scope, context and purposes of the processing). The Agency would maintain a record of all such risk processing activities in the country.

**Special Requirements for Data Protection Officers ("DPO")**

Only individuals who meet the locally set criteria can act as DPOs, in particular: the DPO shall be fluent in the North Macedonian language, shall have a completed higher educational degree and may not be impeded by a sentence, court order or administrative sanction from practicing a specific profession.

As general recommendations we would single out the following:

- **GAP ANALYSIS** Analysis of the current status and assessment of the compliance level with GDPR.
- **ACTION PLAN** Creation of an action plan with prioritized solutions based on risk classification of gaps identified during the gap analysis.
- **IMPLEMENTATION** Development of policies, procedures, internal documentation. Comprehensive support for the introduction of new or modified processes and measures.
- **TOOLS FOR DATA PROTECTION OFFICERS AND DATA PROTECTION IMPACT ASSESSMENTS** PwC has developed DPO & DPIA tools that support organizations in continuous daily operations and data privacy compliance issues.
- **POST-IMPLEMENTATION AND DATA PRIVACY AUDITS** Check your compliance status after implementation from documentation and practical point of view. Gap analysis and tests of personal data protection systems –people, processes, technology.
- **REGULAR TRAINING AND WORKSHOPS** Carrying out trainings and tailored workshops in personal data protection as part of the data protection organizational measures applied by your company.
- **DATA PROTECTION INTERNAL CONTROLS** Assistance in development of data protection control plan enabling the company to control and continuously improve its data protection environment.
- **CONTINUOUS MONITORING AND SUPPORT** Privacy by design for new changes and implementations.
- **REGULATORY ASSISTANCE** Support in your daily cases related to data protection issues and questions.
- **REVIEW AND ANALYSIS OF NORTH MACEDONIAN LEGISLATION** Analysis of local legislation and assessment of compliance level in your organization.

- **DPOs must:**
  - inform and advise the highest level of management and employees about obligations to comply with the Law;
  - monitor compliance with the Law, and with data protection policies, including managing internal data protection activities, raising awareness of data protection issues, training staff, and conducting internal audits;
  - advise on, and to monitor, DPIAs;
  - cooperate with the DZLP; and
  - be the first point of contact for the DZLP and for individuals whose data is processed (employees, customers and others).

## A1. QUESTIONNAIRE FOR THE FOCUS GROUP DISCUSSION

Focus Group Guide

**TI Macedonia**

**18.05.2021**

**Project: COMPLIANCE WITH THE ANTI MONEY LAUNDERING REGULATIONS AND WITH DATA PROTECTION OBLIGATIONS WHEN PROCESSING PERSONAL DATA**

Explanation of the FG discussion

Qualitative research is often used for policy and program evaluation, since it can answer certain important questions more efficiently and effectively than quantitative approaches. This is particularly the case for understanding **how and why** certain outcomes are achieved.

Qualitative researchers aim to gather an in-depth understanding of a behaviour and the reasons that govern such behaviour. The qualitative method examines the *why, what* and *how*, not just *what*, *where*, and *when*. Therefore, smaller but focused samples are more often needed, rather than large, random samples.

Qualitative researchers may use different approaches in collecting data. These can include interviews and group discussions, observation and reflection, field notes, various texts, pictures, and other materials.

One of the central issues in qualitative research is **validity** (also known as credibility and/or dependability). There are many different ways of establishing validity, includinginterviewer validation, peer debriefing, prolonged engagement, negative case analysis, auditability, confirm ability, bracketing, and balance.

In this respect, quality policy is usually based on research of the current state of affairs, **which needs to go beyond popular knowledge and must be as much as possible sector-specific**.

Who: We will invite 6 Categories of participants for the FG Discussion:

1. Private sector Banks – One big bank representative
2. FIU
3. Law Enforcement – ministry for the Interior
4. Prosecutors
5. Judiciary

6. Central Registry
7. Supervisor – Data Protection Agency

FG Guide questions

Who

1. In your view, who is responsible for implementing the Data protection obligations arising from the 5th AML Directive

   In your view who will be the most responsible institution to address the 5th AML Directive requirements for the Data Protection?

   Has your institution already identified the areas of it's responsibilities? Can you say something about it?

What

2. What exactly is the responsibility of your institution?

3. We will also explore what the institutions did in a case, and what happened after the policy decision is taken.

   What your institution did? What was your approach?

   - Adoption of a law, rulebook, guidance, training

   Why you decided to take that approach?

   When?

   What was the level of decision making?

   What happen after you took the initiative/action?

   Are you satisfied with the result?

How?

4. We will also examine what are practical tactics and approaches that can be applied and check why FG participants think an approach will be more successful that the other in data protection in AML procedures.

   We will explore how the officials actually go about data protection observing

   - How is the procedure determined?
   - How is the decision making process designed?

   Which approach you consider to have capacity for being the most successful in data protection?

   What will be the best for the citizen who has nothing to do with the investigation?

Why you believe that approach is better than other is?

Procedure in an individual case / examples

5. We will also explore what the individuals in the institutions do in a specific case, why they did it and what happened after the action they took.

6. Can you explain the procedure in an individual case (give an example)

## A2. CROSS BORDER COOPERATION IN AML/CTF ISSUES

**North Macedonia**

**Skopje, May 2021**

# INTRODUCTION

The new directive (Directive (EU) 2018/843) on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing (the "**5th AML Directive**") amending the 4th AML Directive was published in the Official Journal of the European Union on 19 June 2018, and will enter into force 20 days thereafter. Member States are required to implement the 5th AML Directive into national law by 10 January 2020.

On 12 November 2018, the Sixth AML Directive was published in the Official Journal of the EU. This directive will need to be transposed by the members states by 3 December 2020.

Amongst others, the Sixth AML Directive includes a unified list of predicate offences. These offences refer to the criminal activity that gives rise to, or underpins, a money laundering offence. The directive mentions 22 predicate offences which may generate criminal property for the purposes of committing a money laundering offence. They include environmental crimes, tax crimes and cybercrime, trafficking of drugs and humans and fraud. Directive will increase the workload of compliance officers.

Money laundering and terrorist financing (ML/TF) harm society in a number of ways. Money laundering facilitates and perpetuates crime and supports criminals. Terrorist financing facilitates the commitment of atrocities at home and abroad.

ML/TF cannot be fought in isolation. Governments, public authorities and the private sector all have a role to play. Since its inception, the European Banking Authority (EBA) has been working to foster a common approach by national competent authorities and financial institutions across the single market to anti-money laundering and countering the financing of terrorism (AML/ CFT), and to equip them to apply this approach effectively. A common approach is important, because financial crime respects no borders and a weakness in one area of the single market opens up the entire single market to abuse.

The high-profile scandals of the last few years have shown that, collectively, we must strengthen Europe's AML/CFT defences. It also gave us a new objective, to prevent the use of the financial system for the purposes of money laundering and terrorist financing.

## The key aspects of the 5th AML Directive are:

- an extended scope of the persons subject to the anti-money laundering and counter terrorism financing requirements (in particular to address terrorism financing risks linked to virtual currencies and anonymous prepaid cards and the constant technological evolutions in such field);
- enhanced customer due diligence measures (in particular in the context of financial transactions involving high-risk third countries);
- new increased transparency measures (including enhanced access (for some even public!) to BO registers and through central registries of bank and payment accounts holders at Member State level); and

- enhanced powers for the relevant supervisory authorities and the EU financial intelligence units.

The North Macedonian banking sector is fully committed in the fight against money-laundering and financial crime. For this fight to be effective we need to reduce fragmentation between national approaches while increasing cross-border cooperation in- and outside the European Union.

## Improved Coordination on AML/CTF Data Analysis

The Commission proposes to strengthen the coordination between Member States' Financial Intelligence Units (FIUs). FIUs, which are independent bodies.

Currently, the efficacy of these analyses is undermined by the limited information exchange occurring among FIUs and their failure to take joint actions. The Commission proposes to create an EU-level mechanism to support the work of FIUs and foster coordination among them, enabling collective efforts to identify suspicious cross-border transactions, to carry out joint analysis and to detect trends and factors relevant to AML/CTF.

## International Outreach of EU AML/CTF Efforts

The Commission confirms the EU's ambition to be a prominent international actor in shaping and reinforcing AML/CTF standards while assertively protecting the EU's financial interests.

In this regard, the Commission published a **revised methodology** for identifying high-risk third countries whose AML/CTF rules and practices are deemed a threat to the EU financial system. In applying this methodology to identify high-risk countries, the Commission will (1) examine factors such as each country's practice in enforcing AML/CTF and in cooperating and exchanging information with foreign authorities, (2) work closely with Member State experts and (3) involve the European Parliament and the Council of the EU.

## Conclusion

The Northern Macedonia with the adoption of the current draft Law on Prevention of Money Laundering and Financing of Terrorism is well on its way to harmonization with EU directives, especially with 5$^{th}$ EU Directive.

What needs to be done is the following:

- Streamline supervisory structure;
- Better enforcement of AML directives, proper benefit/cost analysis for new rules;
- Need for Public-Private Partnerships (PPP) and at national level;
- Identifications tools Ultimate Beneficial Owners (UBO) and Legal Entity Identifier (LEI) to be more widely used;
- Develop risk based AML;
- Allow for information exchange private sector;
- Get more date on ML and related crimes;
- Create a cooperation framework ;
- Enhance EU wide coordination cooperation and exchange of information;

- Harmonize definition of crime offence; and
- Align criminal procedures.

151. Countries performed poorly in respect of SR.III, with 24 countries (82.7 %) receiving ratings in the lower range and none were rated as “compliant”. More than a quarter of MONEYVAL countries were found to be “non-compliant”. This is problematic in terms of the general readiness of jurisdictions to freeze terrorist assets. Progress on this issue should be addressed with particular care in the 4th round.[106]

275. In other MONEYVAL countries (Azerbaijan, Croatia, “the former Yugoslav Republic of Macedonia”, Liechtenstein, Lithuania, Moldova and San Marino) there are gaps in the framework for the exchange of information. This is mainly related to the lack of an appropriate legal basis for supervisory authorities to cooperate and share information on money laundering and the financing of terrorism issues, at times hampered by financial secrecy provisions (e.g. Armenia). Some countries have put in place MoUs but it appeared difficult for the evaluators to determine whether such MoUs do provide for the exchange of information related to money laundering and the financing of terrorism beyond the exchange of supervisory information for prudential purposes. Most countries however maintain that requests for information are often forwarded to their financial intelligence unit for the necessary action.[107]

279. The overall ratings for SR.III show that the majority of MONEYVAL countries (16 or 55.2 %) are ‘partially compliant’37. None are ‘compliant’ with 8 (27.6 %) countries[108] falling within the ‘non-compliant’ rating and 5 within the ‘largely compliant’ rating.

[106] Horizontal review of MONEYVAL’s third round of mutual evaluation report, December 2010 cover03.cdr (coe.int)
[107] Horizontal review of MONEYVAL’s third round of mutual evaluation report, December 2010 cover03.cdr (coe.int)
[108] Armenia, Azerbaijan, Bosnia and Herzegovina, Croatia, Moldova, Montenegro, Serbia, “the former Yugoslav Republic of Macedonia”.

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

TRANSPARENCY INTERNATIONAL MACEDONIA

# HOW THE ANTI MONEY LAUNDERING REGULATIONS RESPECT THE DATA PROTECTION IN KOSOVO

**Ehat Miftaraj**

**Yll Zekaj**

**May 2021**

**Kosovo**

I. Glossary....97
II. Introduction....99
III. Methodology....101
IV. Executive summary:....102
V. Legislation on preventing and combating money laundering....103
V.1. Kosovo's legislation on preventing and combating money laundering consists of these acts:....103
V.2. Legislation development....103
V.3. Financial Intelligent Unit (FIU)....104
V.4. Level of approximation with 4th and 5th Directives....105
V.5. International cooperation....107
V.6. Personal data collecting....108
V.7. Inter-institutional cooperation....109
V.8. Inter-institutional cooperation....110
VI. Data protection legislation....112
VI.1. Data protection Commissioner....114
VI.2. Legislation development....114
VI.3. Level of approximation with Aquis communitaire....114
VI.4. AML legislation vis-à-vis Data Protection....115
VI.5. Institutional approach and aspects....116
VI.6. Material approach and aspects....117
VII. Findings....118
VIII. Conclusions....119
IX. Recommendations....120

# I. GLOSSARY

| | |
|---|---|
| TF | Terrorist Financing |
| ML | Money Laundering |
| LPS | Law No. 04/L-155 On Payment System |
| *LPMLCTF* | *Law No. 05/L-096 On the Prevention of Money Laundering and Combating Terrorist Financing* |
| LEPOCOA | Law No. 04/L-140 On Extended Powers for Confiscation of Assets Acquired by Criminal Offence |
| LEDISFIK | Law No.03/L –216 On The Establishment Of A Deposit Insurance System For Financial Institutions in Kosovo |
| *LCISC* | *Law No.03/L –178 on Classification of Information and Security Clearances* |
| *LBMIFJ* | *Law No. 04/L-093 On Banks, Microfinance Institutions and non bank Financial Institutions* |
| FIU-K | Financial Intelligence Unit of Kosovo |
| EU | European Union |
| DNFBP | Designated Non-Financial Business or Profession |
| Directive 2006/70/EC | Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence and for exemption on grounds of a financial activity conducted on an occasional or very limited basis |
| Directive 2005/60/EC | Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing |
| *CPC* | *Criminal No. 04/L-123 Procedure Code* |
| CDD | Customer Due Diligence |
| *CCRK* | *Code No. 04/L-082 Criminal Code of the Republic of Kosovo* |
| AML/CFT | Anti-Money Laundering/Combating (or Countering) the Financing of Terrorism |
| AIP (IAP) | Information and Privacy Agency |
| 5th Directive | Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU |
| 4th Directive | Directive (EU) 2015/849 OF The European Parliament And Of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. |

# II. INTRODUCTION

The justice system in the Republic of Kosovo underwent several judicial reforms since the proclamation of its independence in 2008, which included also enactment of new legislation, most of the time having as catalyzer different external processes such as Visa Liberalization or Stabilization Association Process Dialogue between Kosovo and European Union. The international community and donors have had a major role in successive legislative changes and most of the legislation is aligned with accepted standards and best practices of democratic countries governed by the Rule of Law.[109]

Kosovo adopted its Constitution and various new laws, while at the same time part of the legal framework was inherited from UNMIK which administered Kosovo throughout the previous decade, between 1999 to 2008.

"Within the framework of the two phases of the EU/CoE Project against Economic Crime in Kosovo (PECK I and II), two assessments on "Compliance with international standards in the anti-corruption area" (CoE AC Assessment) and on "Compliance of Kosovo with intentional anti-money laundering and combatting the financing of terrorism standards" (CoE AML/CTF Assessment) were conducted pursuant to CoE evaluation methodologies." [110]

The findings of these assessments have supported some notable improvements and have provided local authorities with a blueprint of steps to be taken to ensure conformity with relevant international benchmarks. Furthermore, several capacity building inputs were provided by previous rounds of PECK in concrete areas, including strategic analysis and risk assessments in the AML, anti-corruption and anti-money laundering criminal procedures and case management, as well as international networking activities.[111]

Challenges however remain. Kosovo needs to further adjust its anti-corruption and AML/CFT regulatory framework in select areas and, more pressingly, needs to boost effective application of anti-corruption and particularly AML/CFT efforts, especially with regard to the approximation of the legislation with EU Directives, and in line with the Kosovo obligations that derive from the Association Stabilization Agreement between Kosovo and EU.

European Union AML/CFF regimes, and especially the Directive 4 and Directive 5 will have a direct impact on the development of the legislative and institutional framework in these regards in Kosovo. It will further affect individuals and financial and business sector. It is therefore paramount that the developments are closely analyzed from the prospective of the existing data protection frameworks. Moreover, European Commission itself highlighted in a July 2019 press release – that AML and other financial crime regulations drastically lack harmonization, whether it be across the EU Member States or between the EU and third countries.

The most prominent measures of AML/CFT are supposed to be based on balance with the personal data protection as a basic human right. This human right is also embedded in to the all-respective countries Constitutions and is frequently observed from the prospective of the need to enhance fight against the organized crime, to control illicit financial flows and money laundering and to ensure safety and security via more effective exchange of data and information. Based on the requirements and frequent assessments of the new typologies and trends all AML/CFT subject seem to agree that the whole point behind compliance efforts is ultimately to serve the general welfare of humanity. Still, one may argue where the limits of the "general interest/common good" umbrella end.

[109] Functional Review of the Justice Sector in Kosovo, Ministry of Justice, November 2020
[110] CoE funded Project: Project against Economic Crime in Kosovo (PECK III)
[111] CoE funded Project: Project against Economic Crime in Kosovo (PECK III)

This report provides current state of play in Kosovo regarding the applicable legislation and established practices in fields of the AML and Data Protection, their approximation with EU Directives, based on the initial assessment completed based on the legislation and secondary literature. This includes both qualitative and quantitative data. The assessment was abased also through comprehensive interviews with 14 stakeholders from public and private sector in order to get to the root of the phenomenon. Also part of the report are insights of cooperation between the countries of the Western Balkans as well as to outside of the region, the practice of the European Court for Human Rights also was assessed and analyzed as well as existing national court judgments where the financial investigation is conducted and confiscation is administrated.

## III. METHODOLOGY

The research it is twofold: first, an initial assessment was completed based on the legislation and secondary literature. This includes both qualitative and quantitative data. After that, two experts conducted interviews in order to get to the root of the phenomenon. In a total of 14 interviews with all stakeholders involved (i.e. prosecutors, bank employees, representatives of financial intelligence institutions, chambers of commerce, Anti-corruption agencies etc.), the local researchers gathered insights of cooperation between the countries of the Western Balkans as well as to outside of the region. The judgments of the European Court for Human Rights were also assessed and analyzed as well as existing national court judgments where the financial investigation were conducted and confiscation was administrated. Therefore, in an attempt to limit the abovementioned modelling problems, one additional international human right expert also scrutinized the existing anti-money laundering practices in the four countries, including Kosovo in order to uncover the failures to address the issue of data protection both in the regulation and in practice. The final assessment will present the regulatory and practical aspects of the data protection in relation to AML/CFT regimes in North Macedonia, Albania, Montenegro and Kosovo and will analyze its main features.

# IV. EXECUTIVE SUMMARY:

Despite the fact that the Republic of Kosovo is not a member state of the European Union, the obligation to approximate national legislation with that of the EU is an international obligation of Kosovo, obtained through the Stabilization and Association Agreement between the European Union and the European Atomic Energy Community, of the one part, and Kosovo, of the other part (Article 74).

In line with this, Kosovo institutions through support and assistance of the international stakeholders, adopted very good legislation in both fields in AML and Data Protection, based on the international and EU standards and practices. Despite advanced legislation, its implementation into practice it is still in very early stage. Although work has started on addressing the flaws in the legal and institutional framework, new changes to the Law on Money Laundering and Terrorism Financing needs to be adopted to bring it fully in line with the EU acquis and international standards. The fight against money laundering and terrorist financing is not efficient enough to produce convincing results. Money laundering is often not prosecuted as a standalone crime, but in connection with other criminal offences, which slows down the overall criminal procedure. There is a pressing need to foster prosecutors' and judges' better understanding of the concept of money laundering and to improve specialization in this field. Based on the EU Country report for Kosovo, during 2019, the FIU received a total of 1,017 suspicious transaction reports. There were 644 such reports in 2018, meaning reports have increased by 58%. In one notable case, FIU intelligence analysis led directly to the conviction of two suspects and final confiscation of nearly EUR 1 million during 2019.

On personal data protection, the law remains broadly in line with the EU General Data Protection Regulation and the Law Enforcement Directive. It envisages compliance inspections, which should be carried out. Finalizing the process of appointing a commissioner to lead the new Information and Privacy Agency – to be selected by the Assembly based on merit and competences – is a crucial first step towards making the Agency operational. In addition, the adoption of new, duly updated, implementing legislation that is aligned with the EU acquis is necessary. Both of these steps are crucial in order to effectively implement the legislation governing personal data protection and access to documents.

The lack of efficiency and professionalism of the judges, prosecutors and law enforcement agencies in implementation of the legislation often it is translated into the lack of legal certainty and concrete results.

# V. LEGISLATION ON PREVENTING AND COMBATING MONEY LAUNDERING

## V.1. Kosovo's legislation on preventing and combating money laundering consists of these acts:

The legislation of the Republic of Kosovo (Republic of Kosovo's legislation) in the field of prevention and combating money laundering is governed by Law No. 05/L-096 on the Prevention of Money Laundering a Combating Terrorist Financing, which entered into force on June 15, 2016.

Kosovo in order to implement the primary legislation, adopted the following secondary legislation:

I. Administrative Instruction on National Money Laundering and Terrorist Financing Risk Assessment;

II. Administrative Instruction on Procedure for Applying Administrative Sanctions For Non-Compliance Of Reporting Subjects With LPMLTF;

III. Administrative Instruction on Politically Exposed Persons.

In addition to this primary and secondary legislation, in order to prevent and combat money laundering, provisions of this nature are also found in other legislation such as:

(i) LBMINBFI

(ii) CCRK

(iii) CPC

(iv) LEPOCOA

(v) LEDISFIK

(vi) LPS

Whereas, in terms of personal data protection, the main law in this area is LPPD. LPMLCTF is also referred to in this law. In terms of the level of compliance with the 4th and 5th directives and compliance with protection of personal data legislation, the most important laws are LPMLCTF and LPPD.

## V.2. Legislation development

Since 1999, Kosovo has been administered mainly by United Nation Mission in Kosovo (UNMIK). Along with UN Resolution 1244, the most important legal document in Kosovo was the Constitutional Framework for Provisional Self-Government in Kosovo, adopted during 2001 by Kosovo Assembly.

In the field of prevention of money laundering, UNMIK on 5 February 2004 approved Regulation No. 2004/02 On the Deterrence of Money Laundering and Related Criminal Offences. This regulation was in force until November 24, 2010, when after the declaration of independence in 2008, the Assembly of the Republic of Kosovo approved Law No. 03/L-196 On the Prevention of Money Laundering and Terrorist Financing. This law was supplemented and amended on March 23, 2013, through law No. 04 / L-178. Whereas, on June 15, 2016, LPMLCTF entered into force.

Regarding the secondary legislation to implement the LPMLCTF, three (3) administrative instructions listed in part V.I. were adopted at the time of the previous law. One of these three (3) administrative instructions (Administrative Instruction Mof– No.04/ 2018 On National Money Laundering and Terrorist Financing Risk Assessment) has already been abolished through the approval of the new

administrative instruction, while the two (2) other administrative instructions of the previous law are still applied under Article 68 of the LPMLCTF[112].

## V.3. Financial Intelligent Unit (FIU)

The Government of Kosovo has made progress with institutional arrangements against money laundering. The Financial Intelligence Unit (FIU) was established in 2010 and administratively it is placed under the Ministry of Finance. The FIU is responsible for requesting, receiving, analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering and terrorist financing. The FIU's Oversight Board is chaired by the Minister of Finance and includes the Minister of Internal Affairs, the Chief State Prosecutor of Kosovo, the Director-General of the Kosovo Police, the Director of the Tax Administration of Kosovo, the Director-General of the Customs and the Governor of the Central Bank of Kosovo. The Board carries out coordination for state-level anti-money laundering (AML) and terrorism financing policy in cooperation with other institutions and relevant stakeholders, and meets at least twice a year.[113]

International conventions and Financial Action Task Force (FATF) recommendations require the inclusion of a number of offences as predicate offences for money laundering such as terrorism, including terrorist financing, trafficking in human beings and migrant smuggling, illicit arms trafficking, environmental crime, fraud, corruption or tax crimes. However, these categories are simply listed and not defined, leaving wide scope for national differences in the range of predicate offences. With this regard the legislation of Kosovo for criminalization of money laundering uses so called "All serious crimes" approach or "list" approach to predicate crimes, which also includes corruption crimes.[114]

In 2018, the FIU has carried out the National Risk Assessment, in which while identifying threats and risks has also handled corruption. A close working group have listed actions for national and sectional risk assessment. Anti-Corruption Agency along with other relevant institutions was involved in this process.[115]

FIU-K has also adopted an Administrative Instruction on Politically Exposed Persons (PEP), aiming at effectively managing the increased risk of money laundering posed by politically exposed persons, in the implementation of provisions on politically exposed persons in accordance with paragraph 1.33 of Article 2, paragraph 1.11 of Article 14 and Article 22 of the Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing. In 2018, FIU has also published a Study of Money Laundering Typologies in relation to the PEPs. By considering that the issue of PEPs is one of the most important points of intersection between AML and anti-corruption efforts, addressing such important tool should be considered as a good practice.

FIU has drafted the Standard Operational Procedures for intelligence and operational analysis. At the end of 2014 year has been signed a comprehensive agreement on cooperation of exchanged information, risk assessment and coordination between institutions and rule of law agencies on combating and preventing economic and financial crimes. FIU is part of several inter-institutional mechanisms including mechanisms that are related to anti-corruption. FIU and Anti-Corruption Agency have also signed an Memorandum of Understanding.[116]

In 2017, Kosovo Financial Intelligence Unit became a member of Egmont Group. It was found that

[112] LPMLCTF. Article 68.2. "Any agreements entered into or any administrative instructions, directives or guidance that have been issued on the basis of provisions of the Law no. 03/L-196 amended and supplemented by the Law No. 04/L-178 already repealed, shall remain in force until they are amended, supplemented or repealed.".

[113] Policy Document 12, Improving Anti-Corruption Institutional Framework, Functional Review of the Rule of Law Sector in Kosovo

[114] Policy Document 12, Improving Anti-Corruption Institutional Framework, Functional Review of the Rule of Law Sector in Kosovo

[115] CoE funded Project: Project against Economic Crime in Kosovo (PECK II)

[116] CoE funded Project: Project against Economic Crime in Kosovo (PECK II)

the FIU has a good cooperation with the rule of law agencies and other institutions, including the Anti-Corruption Agency and there is no sign of overlapping competencies with them.

FIU has the access to the Registry of Anti-Corruption Agency to obtain information about the asset declarations of the senior public officials, including declaring gifts.

## V.4. Level of approximation with 4th and 5th Directives

As discussed in the V.2. section, the LPMLCTF since 2010 has been amended twice (2). The LPMLCTF approved by the Assembly of the Republic of Kosovo in 2016 intends to implement Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC[117].

This way, the ideation of this law, while there was a preceding law, aimed to approximate the legislation of Kosovo in the field of money laundering with the 4th directive.

Following this law, the Republic of Kosovo has not yet adopted a new law in the field of money laundering, until approximately two (2) years after the approval of this law, the 5th regulation was published, which the member states had to implement by 10 January 2020. In Kosovo's case, this did not happen. Furthermore, in the government platform regarding public consultations, a draft for amending and supplementing this law in terms of implementation of the 5th directive does not appear. However, according the FIU representatives this law is aimed to be amended at later stage, during 2022 or 2023, as it was planned in cooperation and coordination with the government and key stakeholders from international community. Such approach it also in line with the Kosovo obligations regarding the implementation of the Stabilization Association Agreement between Kosovo and EU.

Despite the fact that the Republic of Kosovo is not a member state of the European Union, the obligation to approximate national legislation with that of the EU is an international obligation of Kosovo, obtained through the Stabilization and Association Agreement between the European Union and the European Atomic Energy Community, of the one part, and Kosovo, of the other part (Article 74).

The Assessment Report on Compliance of Kosovo With International Anti-Money Laundering And Combating The Financing Of Terrorism Standards has found that, in addition to implementation, in some areas, this directive has been implemented partially, whereas in other cases this directive has not been implemented at all. According to this report Kosovo legislation only partially ensures appropriate steps are taken for overall risk assessment by the obliged entities. There is no general requirement that the steps taken by the obliged entities should be proportionate to the nature and size of the entities (apart from the banks and financial institutions) and no requirement for documenting. The policies, controls and procedures to be applied by the reporting entities are similarly affected by a number of deficiencies (see also below). It cannot be considered that there are adequate safeguards for the application of third-party reliance. The provisions prohibiting the use of anonymous accounts and safe-deposit boxes are broadly in line although the aforementioned general deficiencies with regard to the CDD would negatively impact the measures adopted for safe-deposit boxes. Bearer share warrants are not covered by the prohibition of bearer shares as required by the Directive. A significant deficiency is noted in view of the lack of specific requirements to mitigate the risks associated with electronic money. There are no specific obligations in Kosovo law

[117] LPMLCTF. Article 1.3.

for legal persons and arrangements to obtain and hold information on the beneficial ownership and there are no centralized mechanisms (registers) for holding and making available such information. There is a lack of effectiveness of the application of CDD measures due to the lack of understanding of the beneficial ownership concepts and requirements. Furthermore, with regard to DNFBPs there are major deficiencies in CDD application regardless of the risk. The obligation to report suspicious transactions is limited to the reasonable grounds to suspect proceeds of criminal activity thus omitting knowledge. The reporting obligation would be limited by the deficiencies in regard to the criminalization of ML and TF. The reporting of STRs is (potentially) limited by some discrepancies in the law (especially for DNFBPs). There are some concerns expressed by the assessors with regard to the quality of the reports. The level of reporting is highly uneven, with most of the entities outside the banking sector rarely filing a report. The tipping-off requirements are broadly met. However, it is not clear whether the prohibition under the AML/CFT Law would apply to all employees of the reporting entity filing the report. Limitations are in place to disclose reports to supervisors. The notification/disclosure to the court allowed under the law would not be in line with the requirement of the Directive in all cases. Derogations required by the Directive are mostly not implemented as intended in the Directive. Kosovo legislation is compliant to a large extent with the requirements of the Directive for processing personal data with some minor deficiencies. The AML/CFT Law provides for the requirement for the obliged entities to ensure that the documentation and following information are ready and available to FIU and to other competent authorities, although not in all cases (specifically for DNFBPs) using secure channels and in a manner to ensure the confidentiality. The AML/CFT Law requires maintenance of statistics by all competent authorities with the purpose to enable the FIU to review the effectiveness of the AML/CFT system. There are no legal obligations for the other institutions as to the categories of information needed and for the consolidation of this information as to ensure a meaningful review of the system[118]. This report was published in December 2018. Since then, there has not been any other assessment on the compliance of the legislation with EU directives. In this regard, Kosovo still does not have an assessment of the compliance of the legislation with EU law.

On the other hand, the reason why the new legislation following the 5th EU directive has not been implemented is also due to the political situation in Kosovo, which consists of institutional instability, in last three years.

Mr. Behar Xhema, Deputy Director of the FIU in Kosovo, states that Kosovo is in line with European standards in terms of technical compliance with the FATF recommendations. But the problem still lies with a large number of reporting entities not making a good identification of the beneficial owner. Therefore, explains that they are in the process of drafting the administrative instruction, where the reporting entities must strengthen the measures for the identification of the beneficiary owner until the issuance of the law on the register of the beneficiary owner which is being drafted. While a strong supporter of that law is the Financial Intelligence Unit (FIU). Moreover, the identification of politically exposed persons is very well regulated by the Law on Prevention of Money Laundering and the administrative instruction and Banks also have a special register of banks for politically exposed persons.[119]

One of the registers that serves banks for the identification of politically exposed persons is the register of declaration of assets at the Anti-Corruption Agency. This is only a form of identification; the other form is the very statement made in the bank by politically exposed persons given at the moment the accounts are opened stating that he is a politically exposed person or is a family member of a politically exposed person. In conclusion, Mr. Xhema states that in terms of infrastructure,

[118] See: The Assessment Report On Compliance Of Kosovo With International Anti-Money Laundering And Combating The Financing Of Terrorism Standards. PECK II. December 2018. F. 215-319.

[119] Focus Group discussion held on 14 May 2021

whether it is effective or technical, for the beneficiary owner some amends are needed, a small change in politically exposed persons. While on the protection of personal data it is understood that we take all measures required.[120]

In other hand, there are no regulations or internal acts regarding the protection of personal data withing the SPRK, but the same are obliged to apply them in practice and their daily work in accordance with legal provisions.[121] Mr. Dema believes that there is no need for regulations since it's the law that determines the development of the procedure. Furthermore, the SPRK does not have an official person specializing in personal data protection. But it has an excellent communication and cooperation with the FIU. The FIU sends information directly to the prosecutor handling a case for which the FIU has information including cooperation in conducting joint analyzes and evaluating the case which is being investigated. Usually there is no special form of communication with the FIU, communication is done through personal form of communication "in persona". It is more explained that depending on the complexity of the investigation, they receive information from the FIU and additional information is provided by the FIU from sister agencies that the FIU has in other countries. In the interest of investigations, in addition to information from the FIU, the SPRK also receives information from other reporting entities such as banks and other financial institutions directly, but also from any other institution which may have useful information related to the case. Mr. Dema continues by mentioning how the FIU sends them analyzed and processed information about those transactions. The SPRK has no obligation to notify the FIU of the outcome of investigations in cases where FIU has cooperated, but nevertheless we keep them informed of the indictment and the epilogue of those cases where there was cooperation between the two institutions. The data in the case file are kept until the criminal procedure is finalized at the court and judgment it is final. Afterwards, the case file is archived at the SPRK archive.

*Mr. Kreshnik Radoniqi*, judge at the Appeal Court regarding the money laundering cases declares that within the special Department of the Court of Appeal there have not been many money laundering cases, they had two or three that were completed. He states that there are no unique positions regarding the issue of interpretation of the Law on Money Laundering, but in the cases, they encounter such problems, cases are turned to the Supreme Court to give its opinion. Regarding money laundering, if the prosecution has a different opinion, they have the right to file charges, but the decision will ultimately be made by the court according to how it interprets the law. If there are any differences, again, the Supreme Court gives the opinion. He then adds that there has not been any problem we have faced with the Financial Institutions. Any order issued by the court is immediately implemented by the financial institutions. Each court has an official who has been affiliated with the Central Bank and the orders have gone through him, the banks have had liaison with that court official where there has been an order from the courts.

## V.5. International cooperation

While Kosovo is not party to most multilateral treaties governing mutual judicial cooperation, it unilaterally applies internationally recognised treaty standards. Kosovo's international legal cooperation in criminal matters is based on the relevant 2013 law on international legal cooperation in criminal matters as well as on 28 bilateral treaties. Co-operation with countries with which Kosovo does not have bilateral agreements is based on the principle of reciprocity.[122]

Based on the Law on International Legal Cooperation in criminal matters but also laws that regulate international legal cooperation in general, for any request relating the disclosure of the financial data,

[120] Focus Group discussion held on 14 May 2021
[121] Focus Group discussions held on 14 May 2021
[122] European Commission Country Report for Kosovo for 2020

the request shall go through the competent basic court in Kosovo. Within each Basic Court and Basic Prosecution Office there are trained and specialized judges and prosecutors in processing requests for international legal cooperation. The number of requests for international legal cooperation in this field are minor.

The incoming requests for MLA are handled in Kosovo through a centralised mechanism that in many cases is affected by issues which are detrimental to the effectiveness. The procedures involve the central authority in the Ministry of Justice but also provide for certain requirements for the use of diplomatic channels.

Prosecutor Armend Hamiti, prosecutor at the Basic Prosecution Office in Pristina, it is also the national coordinator for international legal cooperation and also seconded prosecutor to the European Network for Prosecutors and contact person for Kosovo with EJN stated that there are very rare cases of cooperation between Kosovo and other countries in exchanging information regarding the disclosure of financial data that are subject of the international judicial cooperation. He stated that within the Kosovo Prosecutorial Council there is specialized official for Protection of Personal Data, which is competent mainly for documents that are processed by the Prosecutorial Council and doesn't apply for the prosecution offices also. In this regard, each prosecutor is obliged that for his cases to consider and respect the legal obligations regarding the data protection.

With regard to the implementation of the AML, according to him one of the main constraints in implementation and application of a more result-oriented approach required because of the new legislation were the highly technical issues contained in the topics of Confiscation and Money Laundering that were difficult for a majority of the prosecutors and judges to accept. Largely due to the historical structure of the legal system in Kosovo the concept of confiscation and AML of criminal assets was not known. The judges and prosecutors were not trained properly in the use of the AML, in practice still there are different approach of the implementation of such legislation by judges and prosecutors as these were not included in their legal studies curricula and therefore, the issue was not seen as important.

Finally, it is stated that the CBK has no international cooperation regarding the exchange of data, this is done through institutions dealing with financial intelligence such as FIU and also through international legal cooperation. As for reporting to FIU, this is done by reporting entities directly, including banks and microfinance institutions.

## V.6. Cross Border Cooperation in AML/CTF issues

The AML/CFT Law provides for the obligation of the banks and other financial institutions to take measures in relation to respondent institutions in the case of cross-border correspondent banking or other similar relationships to obtain and transmit the necessary information to the beneficiary financial institutions in the case of wire transfers and to implement group-wide AML/CFT programs including information exchange policies and procedures.

The Government of Kosovo adopted a five-year National Strategy and Action Plan for the Prevention of and Fight against the Informal Economy, Money Laundering, Terrorist Financing, and Financial Crimes. An Action Plan annexed to the Strategy outlines concrete activities to achieve the specific objectives and implementation goals in the Strategy, identifies which public institution has the primary responsibility for implementation and reporting, as well as provides a timeline and estimated costs for implementation. Both documents are drafted on the basis of the NRA and are to be reviewed regularly. The Government reviews progress achieved vis-à-vis the Strategy's performance indicators every 6 months and again on annual basis. There is also a built-in monitoring process to review and assess the implementation of the Strategy and Action Plan. Additionally, in September 2017 Kosovo

adopted a National Strategy against Terrorism and Action Plan (2018-2022), as well as strategies in the field of combating organised crime and border management.[123]

Due to its geographic position and a large diaspora abroad, Kosovo faces a particularly broad set of risks in relation to the physical cross-border movement of cash and valuables. It is clear that regional and transnational organised crime groups which are involved in managing the narcotics trafficking along the Balkan route are well represented in Kosovo; organised groups are also involved in cross-border smuggling of goods and migrants, as well as human trafficking and arms trafficking. Members of the large diaspora of Kosovars abroad participate and act as organisers of transnational OCGs with ties back to Kosovo. The money laundering which occurs as a result has a significant cross-border element.

The FIU actively engages in international cooperation and information exchange based on its wide powers under the AML/CFT Law, the MoUs concluded with a number of countries and strictly observing the Egmont Group principles as a member of the organisation since 2017. FIU does not need a MoU as a prerequisite for the exchange of information but it has concluded 16 MoUs, including reviews and renewals of MoUs with some countries, demonstrating additional effort to pursue information exchange with its most important regional partners.[124]

The cooperation implemented by the FIU is active and based on both requests and spontaneous information. Cooperation is carried out pursuant to detailed internal guidelines (SOP) which stipulate the appropriate mechanisms for the various forms of exchange of information. Exact timelines are provided in the internal guidelines. As evidenced from data provided to assessors, FIU practice correlates with the internal requirements and international best practices. The cases presented and the discussions allow the assessment team to conclude that the obtained information is widely used. The powers for police cooperation and exchange of information are widely used, but it is not clear due to the absence of specific statistics to what extent they are actually related to ML and TF cases. The cooperation of customs authorities in Kosovo also seems to be very active although rarely linked specifically to ML. It was not demonstrated that CBK would engage actively in international cooperation specifically for ML and TF purposes.[125]

## V.7. Personal data collecting

The competent authorities of Kosovo have access to and use a significant range of information from various sources, both public and private, and the exchange of information is facilitated by a number of MoUs between institutions. At the same time some concerns are related to deficiencies in some of the databases used and the effectiveness of access to the necessary information in certain cases.[126]

An administrative instruction on standards and methods for collecting, storing, using and deleting personal data has been drafted by Kosovo Police declares *Mr. Haliti*. Continues by explaining that all the data that the Police undertakes during its work activities are treated regulated this instruction: their collection, storage, distribution and deletion. There is a responsible office within the Department of Police Personnel which in cooperation with the legal office deals with the nature of personal data protection.  With regard to the processing of cases and cooperation with the FIU, there are SOP in place which are followed by both institutions.

FIU conducts analysis based on a wide range of sources including STRs, UTRs, CTRs and declarations

[123] See: The Assessment Report On Compliance Of Kosovo With International Anti-Money Laundering And Combating The Financing Of Terrorism Standards. PECK II. December 2018.

[124] See: The Assessment Report On Compliance Of Kosovo With International Anti-Money Laundering And Combating The Financing Of Terrorism Standards. PECK II. December 2018.

[125] See: The Assessment Report On Compliance Of Kosovo With International Anti-Money Laundering And Combating The Financing Of Terrorism Standards. PECK II. December 2018.

[126] CoE AML-CTF Assessment Report-Final, 2018

of monetary instruments at border, as well as additional information that could be gathered from any reporting entities.[127]

FIU has access to a number of databases of public institutions although certain limitations are observed either related to the process of access to the information. FIU has direct access to the databases of the Civil Registration Agency (Civil Status, Vehicle registration database, Family tree), Customs (Export/import of goods and services, Declaration of monetary means at border points, Non-declaration of monetary means), Kosovo Registry of Business Organisations and Trade Names (within the Ministry of Trade and Industry) and DRNGO within MPA.[128] FIU has direct access to the Kosovo Registry of Business Organisations and Trade Names. This would also be the main source of beneficial ownership information. However there are a number of issues related to the availability of adequate information on the beneficial ownership in the register for each and every category of entity.

## V.8. Inter-institutional cooperation

The cooperation of Kosovo's Police with the FIU is regular, especially by the financial investigation sector and the anti-money laundering sector. Mr. Haliti further explained that the Kosovo Police and the FIU have defined the procedure on how information is exchanged and signed a memorandum of cooperation where it is regulated the issue of appointing a liaison officer of the police directorate with the FIU, then using the GoAML system that FIU uses for the exchange of information. At the same time, the Police has enabled FIU access to our database "KPIS". In addition, money laundering collaborations with other countries are done through the FIU, as the FIU is a liaison institution with other financial intelligence units in other countries.[129]

Kosovo authorities have developed a number of mechanisms to assess risks from the holistic as well as sectoral standpoint; mechanisms have been set up on a periodic as well as on-going basis. Notwithstanding the range of mechanisms in place, the authorities do not yet have a fully integrated understanding of ML/TF risks stemming from these exercises. A separate NRA and Serious Organised Crime Threat Assessment (SOCTA) have been undertaken, however they have not been fully coordinated, which should be essential for the next update of both documents in 2018. On a sectoral level, several assessments undertaken recently allowed the Kosovar authorities to develop their understanding of the higher risk areas of real estate, NPOs, construction and games of chance, however these should be further deepened and expanded to ensure all major underlying threats, typologies and financial product vulnerabilities are properly covered for these sectors, understood by authorities and properly communicated to the private sector.[130]

Personal Data Protection In the discussion regarding Personal Data Protection Framework vs AML/ Regimes for Kosovo, *Ms. Marmullaku* described the seriousness of FIU in such field. FIU by using a GoAML system to collect and distribute information, has standard operating procedures, for the process of intelligence and analysis. In addition, they made an action plan, a monitoring tool for the implementation of recommendations which were proposed and finally approved by the government on December 24, 2020, with FIU as monitor. This action plan is actually related to the implementation of the recommendations that are in the evaluation of PECK and several initiatives have started based on that, for example the initiative to change the legislation in the field of Anti Money Laundering, that it should be supplemented and improved from a legislative point of view. Also, is initiated an initiative about amended the Law on SPRK, because SPRK currently has the primacy and has the exclusive competence to fight money laundering, and there is a big criticism here since a lot of

127 *Ibid*
128 *Ibid*
129 Focus Group discussions held on 14 May 2021
130 CoE AML-CTF Assessment Report-Final, 2018

cases are blocked in SPRK. The practice of the states is that these cases should be handled through the Basic Prosecution, while the cases that are much more serious should go to the SPRK. In this regard, we as a project have engaged an expert to make an analysis of this issue and to come up with concrete recommendations for the working group.

In the discussion regarding Data Protection Framework vs AML/Regimes for Kosovo, Ms. Vlora Marmullaku. Project Manager of the EU funded PECK Project described the seriousness of FIU in such field. FIU by using a GoAML system to collect and distribute information, has standard operating procedures, for the process of intelligence and analysis. A new draft Law No. 06/L-082 on Personal Data Protection has been adopted by the Kosovo Assembly during March 2019. The law established the Information and Privacy Agency responsible for supervision of rules on personal data protection and access to public documents which supposed to be led by a Commissioner. Due to the fact that the Kosovo Assembly failed in last two years to appoint the Commissioner, the Agency it is not fully functional. During April 2021, the Kosovo Assembly initiated the process of the appointment of the Commissioner. The Commissioner may impose sanctions (fines) for breaches of law. Since 2019, the Kosovo Assembly failed to appoint the Commissioner, which has direct impact in implementation of the law and its competencies.

Also, the Kosovo government for its Legislative Agenda for 2021, has foreseen an initiative to amended the Law on SPRK, because SPRK currently has the primacy and has the exclusive competence to fight money laundering, and there is a big criticism here since a lot of cases are blocked in SPRK. The practice of the states is that these cases should be handled also by the Basic Prosecution Offices, while the cases that are much more serious should go to the SPRK.

Also, in order that the AML to be in line with the EU Directives, there is need for amendment of the Law on Business Organizations, which shall regulate the issue of the beneficial ownership, in order to establish centralized register for the beneficial ownership within the Ministry of Trade, taking into consideration that within the same Ministry operates the Agency for registration of businesses.

Furthermore, in the area of AML/CFT and as a consequence of the findings and recommendations provided in the AML/CFT Assessment Report, two legal initiatives are underway: the preparation of a concept document aiming at amending and supplementing the Law No. 05/L-096 on the Prevention of Money Laundering and Combating Terrorist Financing, which will take into consideration also the 4th Directive provisions with respect to the legal and institutional framework, and the drafting of a regulation on transparency of beneficial ownership. The PECK II Project is also supporting the review of existing regulations on beneficial ownership transparency in Kosovo and proposing remedies on the identified gaps.[131]

Mr. Labinot Preniqi from the Kosovo Central Bank, stated that they have precise standard operating procedures including the Law on Data Protection, the recommendations of the Agency for Information and Privacy and the bylaws of the CBK that guarantee respect for personal information throughout the activity of the CBK. Within the CBK there is a central register of bank accounts. Only those institutions which are allowed by the law of enforcement procedure and only those which have responsibilities for the development of enforcement procedure such as: KJC, private and judicial bailiffs, TAK have direct access to this register. Mr. Preniqi continues by mentioning that every access, every trace, every touch, every login is tracked and the report is issued for every user at what time they have used the system, respectively at what level they have accessed the registry.

[131] Focus Group discussions held on 14 May 2021

# VI. DATA PROTECTION LEGISLATION

In the Republic of Kosovo, protection of personal data is guaranteed by the Constitution of the Republic of Kosovo, which in Article 36.4. states that "Every person enjoys the right of protection of personal data. Collection, preservation, access, correction, and use of personal data are regulated by law." In terms of legislation, the main law governing this area is LPPD.

Kosovo law defines in broad terms the information to be retained but the provision cannot be strictly interpreted as requiring sufficient supporting evidence, the original documents or copies admissible in judicial proceedings under the applicable national law, as required in letter (b) of Paragraph 1 of Article 40 of the Directive.[132] For banks, the CBK regulation solves this issue, but not for other entities. Furthermore, it is not clear whether all information obtained through CDD measures would be subject to the record-keeping requirements. The periods for record-retention are not entirely in line with the Directive. 27. Kosovo legislation is compliant to a large extent with the requirements of the Directive for processing personal data with some minor deficiencies. The AML/CFT Law provides for the requirement for the obliged entities to ensure that the documentation and following information are ready and available to FIU and to other competent authorities, although not in all cases (specifically for DNFBPs) using secure channels and in a manner to ensure the confidentiality.[133]

This law defines the rights, responsibilities, principles, and punitive measures related to the protection of personal data and privacy of the individual. This law defines the responsibilities of the responsible institution for overseeing the legitimacy of data processing and access to public documents[134] and the same applies to the processing of personal data by public and private bodies[135].

The issue of the protection of the personal data in processing the financial data it is not considered an important issue by most of the stakeholders in Kosovo. Additionally, although majority of the institutions have assigned the Data Protection Officers, most of officials within institutions are not aware about it and majority of officials lack information on the role and importance of the data protection officials.[136]

"Personal Data - any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;"[137].

This law defines provisions in relation to the legal processing of personal data, consent conditions, processing of special categories of personal data, information and access to personal data, restrictions, etc.

Regarding the security of personal data, this law states that "Taking into account the technology, the costs of implementation and the nature, scope, context, and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller, and the processor, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk"[138].

Regarding the institutional framework, for the protection of personal data, this law has mandated

132 CoE AML-CTF Assessment Report-Final, 2018
133 CoE AML-CTF Assessment Report-Final, 2018
134 LPPD. Article 1.1.
135 Ibid. Article 2.1.
136 Interview with Bujar Sadiku, Director of the Data Protection Agency
137 Ibid. Article 3.1.1.
138 Ibid. Article 31.1.

AIP. The Agency is an independent authority responsible for overseeing the implementation of this law and other regulations concerning personal data protection and access to public documents and information[139].

In terms of personal data protection, this law has defined tasks and competencies of AIP without harming other duties defined in accordance with this law, AIP performs the following duties: 1.1. supervises the implementation of this law; 1.2. provides advice to public and private bodies on issues related to data protection; 1.3. informs the public on issues and developments in the area of data protection; 1.4. promotes and supports fundamental rights on personal data protection; 1.5. decides about complaints submitted by data subjects; 1.6. provides advice to the Assembly, the Government, other internal institutions, and bodies on legislative and administrative measures in relation to the protection of fundamental rights and freedoms of natural persons in terms of data processing; 1.7. carries out inspections regarding the implementation of this law; 1.8. as appropriate, carries out a periodical review of issued certifications in accordance with Article 43 of the Law and may withdraw certification in case certification criteria are no longer met; 1.9. on its own initiative or upon request it provides opinions for public institutions and other bodies, as well as publishes on any issue related to personal data protection.[140].

According to the LPPD, the AIP may, ex officio or on a complaint basis, conduct inspections and controls to oversee compliance with data protection rules[141].

Bujar Sadiku, Director of the Data Protection Agency, states that the Agency is constantly in contact with all data protection officers, where they have the list on the web and are trying to increase the capacity of data protection officers and professionalize institutions in implementing the new Law on Personal Data Protection. Mr. Sadiku further stated that the institutions of the judicial system do not meet the basic criteria to implement the security measures for data protections that are necessary. After meetings with them and after the recommendation given, they tried and have fulfilled most of them, especially the ones coming from the new law. At the end concludes by saying that the Agency has never had any obstacles with security institutions, except that they had insufficient knowledge, and as a result of this cooperation, the Academy of Justice has been providing training on knowledge on the Data Protection Law every year. We also have very good cooperation with both the Kosovo Police and the FIU.[142]

Mr. Preniqi stated that they have precise standard operating procedures including the Law on Data Protection, the recommendations of the Agency for Information and Privacy and the bylaws of the CBK that guarantee respect for personal information throughout the activity of the CBK. Within the CBK there is a central register of bank accounts. Only those institutions which are allowed by the law of enforcement procedure and only those which have responsibilities for the development of enforcement procedure such as: KJC, private and judicial bailiffs, TAK have direct access to this register. Mr. Preniqi continues by mentioning that every access, every trace, every touch, every login is tracked and the report is issued for every user at what time they have used the system, respectively at what level they have accessed the registry.

In addition, Mr. Bajraktari stated that the Ministry of Justice plays an important role through the drafting of legislation on money laundering. In the framework of criminal legislation reforms, issues related to money laundering and prevention of terrorist financing are addressed and, in this process, institutions that deal with the investigation and combating of these criminal offenses including the FIU have been involved. The Ministry of Justice does not have officials who are specifically appointed to deal with the issue of personal data protection, but it cooperates with Agencies for the protection

139 Ibid. Article 57.1.
140 Ibid. Article 64.
141 Ibid. Article 6
142 Focus Group discussions held on 14 May 2021

of privacy and personal data when it is deemed necessary to consult with them regarding personal data involved in various legislative processes. However, The Ministry of Justice is now in the process of drafting a code of criminal procedure and amendment of the Law on International Legal Cooperation in criminal matters, it will be subject to the process of conformity assessment in EU legislation, and within this laws, the procedures for data protection will be regulated through the investigation and adjudication of criminal cases.

## VI.1. Data protection Commissioner

On personal data protection, the law remains broadly in line with the EU General Data Protection Regulation and the Law Enforcement Directive. It envisages compliance inspections, which should be carried out. Finalising the process of appointing a commissioner to lead the new Information and Privacy Agency – to be selected by the Assembly based on merit and competences – is a crucial first step towards making the Agency operational. In addition, the adoption of new, duly updated, implementing legislation that is aligned with the EU acquis is necessary. Both of these steps are crucial in order to effectively implement the legislation governing personal data protection and access to documents. During April 2021, the Kosovo Assembly initiated the process of the appointment of the Commissioner.

Flutura Kusari and Mexhide Demolli, civil society activists specialized in data protection stated that although Kosovo adopted very advanced law on Data Protection, the issue of the postponement of appointment of the Data Protection Commissioner by the Kosovo Assembly for almost three years, had impact in non-implementation of the same law in line with its spirit.

## VI.2. Legislation development

The 2001 CFPSG stipulated that "The Provisional Institutions of Self-Government shall also have the following responsibilities in the field of judicial affairs (k) Protecting personal data relating to the judicial system and correctional service".

In terms of law, the protection of personal data in Kosovo was initially regulated by the Law on the Information Society Services which was conveyed by the Special Representative of the Secretary-General of UNMIK on 8 May 2006.

After the declaration of independence in 2008, the Assembly of the Republic of Kosovo approved the LPPD, which came into force on 15 June 2010.

Regarding the bylaws, the Government of the Republic of Kosovo on April 4, 2012, had approved Administrative Instruction No. 03/2012 On National Supervisors Identification Cards. Despite the fact that this bylaw was issued based on the already abolished law, the same is still applicable in the sense of Article 109.2. of LPPD[143].

## VI.3. Level of approximation with Aquis communitaire

Regulation 2016/679 of the European Parliament and of the Council abolishes the preliminary directive in this area, namely Directive 95/46 / EC.

LPPD itself has determined that "This Law is in compliance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing

[143] LPPD. Neni 109.2. "Sub-legal acts that are into force shall continue to be applied until the issuance of new sublegal acts, provided that they are not in contradiction with this Law".

Directive 95/46/EC (General Data Protection Regulation)".

Regarding Directive 95/46/EC, Article 64 of law on PML/CTF is largely compliant to article 41 of the Directive. Moreover, the PML/CTF law is in compliance with most of the necessary requirements pursuant to Directive 95/46/EC (e.g. Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) as implemented in Kosovo by the Law on the Protection of Personal Data.

Paragraph 2 of this article is met by paragraphs 2 and 3 of Article 64 PML/CTF law. While paragraph 3 is not explicitly implemented in the Kosovo legislation or regulations. Paragraph 4 of this article is met through the relevant provisions of PML/CTF Law on the "processing and the protection of the data although the manner in which the retention period for data is specified (record-keeping requirements) does not fully meet the requirements for personal data protection"

## VI.4. AML legislation vis-à-vis Data Protection

In terms of legal definition, LPMLCTF and LPPD are harmonized. Furthermore, the LPMLCTF stipulates the obligation to comply with LPPD during data processing. However, the reference is not precise in LPPD, but is general in the sense of "other laws". A phrasing of this nature implies the obligation to implement the Law on *Classification of Information and Security Clearances* (LCISC).

In this regard, Article 64 of the LPMLCTF specifies that "1. FIU-K is a data controller as defined in the Law on the Protection of Personal Data. Pursuant to this Law, information received and kept by FIU-K is processed and administered in accordance with this law and other legislation in force. Collection, processing, use, and record keeping of personal data from reporting entity is limited to what is necessary for the purpose of the action in accordance with the requirements of this law and personal data should not be further processed in a way incompatible with this purpose. In particular, the further processing of personal data for commercial purposes is prohibited.

On the other hand, LPPD has defined the principles of personal data processing. One of these principles is the principle of **purpose limitation,** which principle according to the LPPD means that "data are collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose."[144] Also, among others, this law has defined the principle of storage limitation, where it underlines that - personal data may be stored insofar as necessary to achieve the purpose for which are further collected or processed. After the fulfillment of processing purpose, personal data shall be erased, deleted, destroyed, blocked, or anonymized, unless otherwise foreseen in the Law on State Archives or in another relevant law."[145].

In this respect, what is seen from these legal formulations is that both the LPMLCTF and the LPPD define more general terms, and do not regulate real situations, but that these principles are left to the FIU-K to apply them on a case-by-case basis. In this case, the principle of purpose limitation in the case of money laundering has a wide applicable scope. This is because the very purpose of LPMLCTF is very broad. " This Law stipulates measures, competent authorities and procedures for detecting and preventing money laundering and combating terrorist financing. " states Article 1 of this law.

In this field, in addition to these two (2) laws, LCISC is also applicable. Article 6 of this law has determined Information may be classified at one of the following levels: 1.1 "TOP SECRET" shall be

[144] Ibid. Article 4.2.
[145] Ibid. Article 4.5.

applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to security interests of the Republic of Kosovo; 1.2. "SECRET" shall be applied to information the unauthorized disclosure of which could seriously damage security interests of the Republic of Kosovo; 1.3. "CONFIDENTIAL" shall be applied to information the unauthorized disclosure of which could damage security interests of the Republic of Kosovo; 1.4. "RESTRICTED" shall be applied to information the unauthorized disclosure of which could be disadvantageous to the security interests of the Republic of Kosovo.

In terms of FIU-K information, the vast majority of data are classified as "Confidential" and "Secret".

## VI.5. Institutional approach and aspects

Regarding the institutional framework, in relation to LPMLCTF has defined the FIU-K as a basic institution mandated for this field, while there are several other institutions that contribute in this area. Regarding the protection of personal data, LPPD has defined Information and Privacy Agency (AIP).

Regarding the connection of these two (2) institutions in terms of personal data protection in the field of preventing and combating money laundering, the laws do not define any special report in addition to the general rapport of the Information and Privacy Agency in terms of personal data protection.

In this sense, IAP's right to protect personal data in the field of preventing and combating money laundering consists of 2 means: AIP authority and the application of legal means.

In terms of AIP's authority, LPPD determines that the IAP, among others: Supervises the implementation of this law, Provides advice to public and private bodies on issues related to data protection, Carries out inspections regarding the implementation of this law, On its own initiative or upon request it provides opinions for public institutions and other bodies, as well as publishes on any issue related to personal data protection etc[146].This article is in compliance with the 29th recommendation of FATF recommendation.

These competencies guarantee the AIP that even in the absence of a complaint, it has the opportunity to proactively protect personal data in relation to all institutions, consequently the FIU-K and other institutions that process personal data. Inspection regarding the implementation of the law that protects personal data, remains one of the main competencies that enables the AIP to protect personal data even in the absence of a complaint. On the other hand, if the AIP finds violations, it also has the power to punish institutions, in this case the FIU-K and other institutions that in the sense of preventing money laundering, process personal data.

Chapter XXI of the Law on Personal Data Protection also defines the punitive provisions for violations of this law. There are a total of 17 articles that define punitive norms for violations of this law, among them Article 105 which notes that "If the Agency find there is a serious and great violation of personal data, it may impose a fine from twenty thousand (20,000) € to fourty thousand (40,000) € or in the case of a company or an enterprise it may impose a fine amounting two percent (2%) to four percent (4%) of the general turnover of the previous fiscal year in compliance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data".

On the other hand, every person who is the subject of the data has the right to appeal to the AIP, if he claims that his rights as defined by law have been violated. In this regard, LPPD stipulates that "1. Without prejudice to other administrative or judicial remedies of protection, any data subject

[146] Ibid. Article 64.

has the right to file a complaint before the Agency, if the data subject claims that the processing of his or her personal data violates this law. 2. The Agency shall notify the complainant of the progress and outcome of the complaint, including the possibility of a judicial remedy in accordance with Article 54 of this Law."[147]. The Law on Protection of Personal Data contains detailed provisions for the processing of personal data. In this case, any person who considers that his rights have been violated through the illegal processing of personal data, can file a complaint to the AIP. The complaint in this case can be against the FIU, as well as other institutions that process personal data in order to prevent money laundering.

Further, the unsatisfied party has the right to initiate an administrative dispute before the competent court against the Commissioner's final decision, more specifically the Basic Court of Pristina, Department for Administrative Matters.[148].

In this case, although in terms of personal data protection there is no specific report, based on the general definitions, AIP has sufficient authority to exercise active supervision regarding the protection of personal data in the field of prevention and combating money laundering.

In this regard, in addition to AIP, the judiciary also appears as a protector of personal data, although due to procedural aspects, it does so at a later time.

## VI.6. Material approach and aspects

As stated above, the LPMLCTF and LPPD in principle, have defined a harmonization between themselves, obliging the FIU-K to apply in relation to personal data, other relevant laws, which in this case LPPD appears as unsurpassed.

But, as already stated above, this definition is initially only in principle, while based on the dispositions of LPMLCTF and LPPD they have a very broad approach in this case, which does not guarantee sufficient legal certainty in terms of protection of personal data in the field of preventing and combating money laundering. LCISC made progression in this case.

In this respect, regarding the protection of personal data in the field of preventing and combating money laundering, despite the importance of measure effectiveness in this area, it is more important to detail the dispositions regarding personal data protection. Based on the way money laundering takes place and the phrasing in LPPD, in almost every case there can be a "definite purpose". These provisions of a general nature give FIU-K rights that have the potential to become arbitrary.

Because of these reasons, in terms of harmonization of the dispositions of the LPMLCTF and LPPD, more details are required in regards to personal data.

On the other hand, based on the provisions of these two laws, AIP is not able to intervene in real-time on each case regarding personal data protection. Due to this, in terms of harmonization of LPMLCTF and LPPD, in certain areas, it is required to be stipulated the obligation of AIP to issue legal opinions for the laws and by laws that regulate legal basis and procedures for personal data use, which obligation should be adapted in a way that does not harm the effectiveness of preventing and combating money laundering.

147 Ibid. Article 52.

148 Ibid. Article 53 and 54; LKA. Article 13; LGj. Article 12.4 and 13.1.1.3.

# VII. FINDINGS

Even though Kosovo adopts very good legislation in both fields in AML and Data Protection, its implementation into practice it is still in very early stage. Although work has started on addressing the flaws in the legal and institutional framework, new changes to the Law on Money Laundering and Terrorism Financing needs to be adopted to bring it fully in line with the EU Directives 4 and 5. Money laundering is often not prosecuted as a standalone crime, but in connection with other criminal offences, which slows down the overall criminal procedure. There is a pressing need to foster prosecutors' and judges' better understanding of the concept of money laundering and to improve specialisation in this field.

Additionally, the other laws such as the Law on Businesses Organizations shall be amended in order that the beneficiary ownership to be regulated in line with the EU Directives. The legislative framework on the prevention of money laundering and terrorist financing in sot aligned with the EU acquis and in particularly with the 4$^{th}$ and 5$^{th}$ AML/CFT Directives . Inter-institutional cooperation to ensure proper investigation and prosecution of offences in that area should be enforced.

On personal data protection, the law on personal data protection remains broadly in line with the EU General Data Protection Regulation and the Law Enforcement Directive. It envisages compliance inspections, which should be carried out by the Information and Privacy Agency once the same it is fully functional and operational. Finalising the process of appointing a commissioner to lead the new Information and Privacy Agency – to be selected by the Assembly based on merit and competences – is a crucial first step towards making the Agency operational. In addition, the adoption of new, duly updated, implementing legislation that is aligned with the EU Directives. Both of these steps are crucial in order to effectively implement the legislation governing personal data protection and access to documents.

The direct access to this national bank register has only institutions which are allowed by the law of enforcement procedure and only those which have responsibilities for the development of enforcement procedure such as: KJC, Private and judicial bailiffs and TAK.

The issue of the protection of the personal data in processing the financial data it is not considered an important issue by most of the stakeholders in Kosovo. Additionally, although majority of the institutions have assigned the Data Protection Officers, most of officials within institutions are not aware about it and majority of officials lack information on the role and importance of the data protection officials.

Identification of politically exposed persons is very well regulated by the Law on Prevention of Money Laundering and the administrative instruction and Banks also have a special register of banks for politically exposed persons.

The Academy of Justice has been providing trainings on the Data Protection Law every year, however, there is an immediate need in providing special trainings for judges and prosecutors oriented towards also data financial data protection.

# VIII. CONCLUSIONS

- Even though Kosovo adopted advanced legislation in AML and Data Protection, further harmonization with EU Directives and EU best practices it is needed.

  Additionally, Kosovo institutions shall take further steps to ensure the implementation of such legislation into practice.

- Identification of politically exposed persons is very well regulated by the Law on Prevention of Money Laundering and the administrative instruction and Banks also have a special register of banks for politically exposed persons

- The direct access to this national bank register has only institutions which are allowed by the law of enforcement procedure and only those which have responsibilities for the development of enforcement procedure such as: KJC, Private and judicial bailiffs and TAK;

- Institutions of the judicial system do not meet the basic criteria to implement the security measures for data protections that are necessary;

- Ministry of Justice does not have officials who are specifically appointed to deal with the issue of personal data protection;

- Agency for Information and Privacy handled trainings for institutions as well as awareness campaigns for the implementation of the Law on Data Protections.

- The Academy of Justice has been providing training on knowledge on the Data Protection Law every year.

- FIU are waiting the formation of the new government, for establishing the working groups to start addressing the analysis the change of the legislation that affects the reform in the field of money laundering and financing terrorism.

- Kosovo Assembly failed to appoint the national commissioner for data protection, which is having impact in functionality of Agency for Data Protection to be operational and to exercise its functions and competencies.

# IX. RECOMMENDATIONS

1. The Assembly of the Republic of Kosovo, in order to ensure full compliance of national legislation with EU Directives, initiates a new Law on Preventing Money Laundering.
2. The Assembly of the Republic of Kosovo amends/supplements the Law on Business Organizations in order to regulate beneficiary ownership in line with EU Directives.
3. In order to prevent and combat money laundering, institutions should advance interinstitutional cooperation.
4. In order to ensure implementation of the Law on Protection of Personal Data, the Information and Privacy Agency should regularly exercise its competence for inspection.
5. The Assembly of Republic of Kosovo, in a merit-based procedure, appoints the Commissioner for Privacy and Information.
6. Public institutions train Personal Data Protection Officers on the role and duties they have.
7. Academy of Justice organizes specialized trainings for judges and prosecutors on the protection of financial data.
8. The new AML Law must contain clear and explicit provisions on the duty to protect personal data.

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

TRANSPARENCY INTERNATIONAL MACEDONIA

# HOW THE ANTI MONEY LAUNDERING REGULATIONS RESPECT THE DATA PROTECTION IN MONTENEGRO

**Biljana Papović**

**Ivan Vukcević**

I. Glossary ..... 113
II. Introduction ..... 114
III. Methodology ..... 115
IV. Executive summary ..... 116
V. AML legislation ..... 117
V.1. Legislation development ..... 117
V.2 Level of approximation with Directive 4 and 5 ..... 118
VI. Data protection legislation ..... 121
VI.1 Legislation development ..... 122
VI.2 Level of approximation with “acquis communautaire” ..... 122
VII. AML legislation vis-à-vis Data Protection ..... 124
VII.1 Institutional approach and aspects ..... 125
VII.2 Material approach and aspects ..... 127
VII.3 Conclusions ..... 127
VIII. Recommendations ..... 130

# I. GLOSSARY

| | |
|---|---|
| MFIU | Montenegrin Financial Intelligence Unit |
| MoI | Ministry of Interior |
| CBM | Central Bank of Montenegro |
| TD | Tax Directorate |
| APC | Agency for Prevention of the Corruption |
| APDP | Agency for Personal Data Protection |
| AMLL | The Law on Prevention of Money Laundering and Terrorism Financing (Anti Money Laundering Law) |
| AMLD | Anti Money Laundering Directive |
| LPDP | Law on Personal Data Protection |
| GDPR | General Data Protection Regulation |
| 4th Directive | Directive (EU) 2015/849 of the European Parliament and of the Council |
| 5th Directive | Directive (EU) 2018/843 of European Parliament and of the Council |
| OSCE | Organization for Security and Co-operation in Europe |
| CoE | Council of Europe |
| EU | European Union |
| LEAs | Law Enforcement Authorities |
| FATF | Financial Action Task Force |

## II. INTRODUCTION

European Union AML/CFF regimes, and especially the Directive IV and Directive V will have a direct impact on the development of the legislative and institutional framework in Montenegro as candidate for membership of the European Union. It will further affect individuals and financial and business sector. Moreover, European Commission itself highlighted in a July 2019 press release – that AML and other financial crime regulations drastically lack harmonization, whether it be across the EU Member States or between the EU and third countries. Also, reports of European Commission on progress of Montenegro emphasize necessity to not only adopt laws that are in line with EU standards, but to implement them so that indicators from Chapters 23 and 24 can be achieved.

The most prominent measures of AML/CFT are supposed to be based on balance with the personal data protection as a basic human right. This human right is also embedded in to the all-respective countries Constitutions and is frequently observed from the prospective of the need to enhance fight against the organized crime, to control illicit financial flows and money laundering and to ensure safety and security via more effective exchange of data and information. Based on the requirements and frequent assessments of the new typologies and trends all AML/CFT subject seem to agree that the whole point behind compliance efforts is ultimately to serve the general welfare of humanity. Still, one may argue where the limits of the “general interest/common good” umbrella end.

Considering that Montenegro is behind the developed EU member countries in establishing appropriate legislative and institutional AML/CFT regimes that will enable more efficient regional and broader cooperation, it will be important to assess the approximation of the existing legislation and regulative frameworks with the 4th EU AML Directive (EU) 2015/849 and the Directive (EU) 2019/1153 with special focus on its consistency with the data protection regulations.

## III. METHODOLOGY

The research was twofold: first, an initial assessment was completed based on the legislation and secondary literature. This includes both qualitative and quantitative data. After that, two experts conducted interviews in order to get to the root of the phenomenon. In a total of 10 interviews with all stakeholders involved (i.e., prosecutors, bank employees, representatives of financial intelligence institutions, chambers of commerce, Anti-corruption agencies etc.), the local researchers gathered insights of cooperation between the countries of the Western Balkans as well as to outside of the region. The judgments of the European Court for Human Rights have also been assessed and analyzed as well as existing national court judgments where the financial investigation is conducted and confiscation is administrated.

The aim of final assessment is to present the regulatory and practical aspects of the data protection in relation to AML/CFT regimes in Montenegro and analyze its main features.

The individual country reports will be presented to the authorities as an input, rather than as country case study and will take a cross-border perspective looking first at AML/CFT Directives and data protection in general, as well as money laundering activities in particular, and their implications on local and regional governance and the economy. This includes a full picture on how the AML/CFT is organized VS the data protection as well as an assessment of the current legislation and the role of the financial intelligence institutions in each country.

# IV. EXECUTIVE SUMMARY

The Law on the Prevention of Money Laundering and Terrorism Financing Montenegro (AMLL) governs the establishment, content, bases of recording and manner of keeping the register of beneficial owners of legal entities and other entities registered in Montenegro. In follow up of the 4th round mutual evaluation report of MONEYVAL which took place in April 2015, amendments were made to LPMLTF, notably with respect to the requirements of the 5th AMLD. The last amendments were adopted by the Montenegrin Parliament on 17 December 2019. The amended LPMLTF regulates the competencies, powers, affairs and organization of the Police-based FIU, including the Protection of data and information kept by it. It also establishes conditions for creating functional PEP lists.

According to MONEYVAL, Montenegro has also made significant progress in addressing many of the identified deficiencies under R.1 (criminalization of money laundering), 3 (confiscation measures), 5 (customer due diligence), 13/SR.IV (suspicious transaction reporting), 23 (supervision), 40/SR.V (international cooperation), SR.I (international conventions on terrorism financing), SR.II (criminalization of terrorism financing) and SR.III (freezing of terrorist funds), which has brought the level of compliance with these recommendations to “largely compliant”. Due to afore-mentioned changes at the legislative level, in May 2020, MONEYVAL formally removed Montenegro from the fourth round’s regular follow-up process, considering that the country had taken sufficient steps to remedy deficiencies that had been identified in 2015.

However, certain elements of the legislation are still not fully in line with the EU directives. The current register of beneficial ownership, including the one that exists within the Tax Administration as well as the Central Register of Business Entities (CRPS) are not fully compliant with the requirements of the 5th AMLD. The register was supposed to be formed last year according to the Law, but due to the amendments to the bylaw that were adopted in December last year, it is planned that the register will be formed in May 2021. There are still no sanctions for a failure to submit requested ownership data. Hence, the identification of the real owners of private companies and tracing of their financial transactions is expected to remain challenging. The plan is to adopt a new AML Law because planned changes will be in more than 50% of the content of the law currently in force. These amendments would also incorporate the 5th Directive. The Government planned to complete the drafting of a new law in the third quarter of 2021.

The Law on Personal Data Protection (LPDP) is harmonized with Regulation 2016/679 of the European Parliament and the Council, as well as Directive 2016/680. However, the question remains as to how successfully the Law is applied in practice. Although the 5th Directive in the field of prevention of Money Laundering is partly related to Data Protection, the Government intends to implement the 5th Directive not through amendments to the Law on Personal Data Protection, but through the new AMLL.

Alignment with the GDPR will be part of new PDP law, planned for IV quarter of 2021, while the Police Directives will be part of the new legal text. This new law also being prepared, in line with Directive 680, which concerns the protection of personal data when it comes to law enforcement authorities. AML law will be harmonized with Directives 680 regarding PDP and 1153/2019 on the manner of using financial data.

# V. AML LEGISLATION

The AML legislation in Montenegro is composed of the following main legal instruments:

(i) Council of Europe Convention on the Prevention of Terrorism[149];

(ii) Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and Financing of Terrorism[150];

(iii) AML Law[151];

(iv) LPD Law;

(v) Law on Central Bank[152];

(vi) Law on Banks[153];

(vii) Law on Confiscation of Property Benefits Gained by Criminal Offense[154];

(viii) Rulebook on the manner of keeping the register of beneficial owners, collection, entry and deadlines of entry and updating of data kept in the register and manner of access to this data

(ix) Sublegal acts issued on applicability of the abovementioned instruments.

The most important acts in the context of this Report regarding of level of approximation with 4th and 5th Directives, and compliance with data protection legislation, are the ones indicated under points (iii) to (vi) above.

Firstly, the AML Law having as scope the prevention of money laundering and products deriving from criminal offences, as well as the prevention of terrorism financing.

AML Law provides for the detailed rules and regulations regarding the AML surveillance, beneficial ownership, risk analysis, risk management, politically exposed persons, categories of personal data being processed (i.e. collected, retained, transferred) for purpose of AML, international cooperation, the categories of persons/entities being subject thereof, AML reporting obligations, functions and responsibilities of MFIU, etc.

Secondly, the LPDP provides for data processing, erasure of data, special types of data processing, Agency for Personal Data Protection (APDP), sanctions.

Thirdly, the Law on Central Bank and Law on Banks, determines duties of CBM and banks regarding AML, the principles of risk management and the obligation of data confidentiality.

## V.1 Legislation development

The following represents a historical outline of the main developments related to the establishment and institutional consolidation of the AML legislation Montenegro.

149 Council of Europe Convention on the Prevention of Terrorism, Warsaw, CETS No.196, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/09000016808c3f55

150 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CETS No.198, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/198

151 Law on Prevention of Money Laundering and Terorism Financing,( Official Gazete no. 033/14 04.08.2014, 044/18 06.07.2018, 073/19 27.12.2019)

152 Law on Central Bank (Official Gazete no. 040/10 22.07.2010; 046/10, 06.08.2010; 006/13, 31.01.2013; 070/17, 27.10.2017)

153 Law on Banks (Official Gazete, no. 017/08, 11.03.2008, 044/10,30.07.2010, 040/11, 08.08.2011, 073/17, 03.11.2017)

154 Law on Confiscation of Property Benefits Gained by Criminal Offense (Official Gazete no 058/15 09.10.2015, 047/19, 12.08.2019)

The Law on Prevention of Money Laundering and Terrorist Financing (AMLL) was adopted in 2007.[155] It regulates measures and actions taken to detect and prevent money laundering and terrorist financing.

The law was subsequently amended in 2008 and 2012 to bring it into line with FATF (Financial Action Task Force) recommendations and other international recommendations.

The new law was adopted in 2014. The main reason for the adoption of the new Law on Prevention of Money Laundering and Terrorist Financing is compliance with the recommendations of MONEYVAL (Measures against Money Laundering and Terrorist Financing at the Council of Europe), New Recommendations of the Working Group on (FATF), Directive 2005 / 60 / EC of the European Parliament and of the Council of 26.10. 2005 on the prevention of the use of the financial system for the purpose of Money Laundering and Terrorist Financing (32005L0060) and Directive 2006/70 / EC of 1 August 2006.

The law was amended in 2018 to harmonize with the 4th Directive of the European Parliament and the Council in the field of prevention of money laundering. In 2019 Law was amendment due to organizational changes in the police administration.[156]

## V.2 Level of approximation with 4th and 5th Directives

The AML Law is almost completely harmonized with the 4th Directive, and Montenegro started to adopt new standards, only a year and a half after the 5th Directive. Amendments to the new Law on the Prevention of Money Laundering are currently being drafted and it is expected to have new draft Law in the third quartal of 2021. The aim of new Law is to adopt changes to align with EU 5th Directive. There is a continuing desire to bring legislation in this area in line with international standards.

The COE provided support to the FIU and the working group for the harmonization of AML Law with the 4th Directive, which was achieved by the current Law. At the same time, standards in the field of personal data protection were considered. Alignment with the 5th Directive is now underway, which is being monitored equally by CoE experts. Initial recommendations have found a place in the new law, in this area the institutions are open to COE proposals, but the problem is how to link it with the overall legislation.

Montenegro legislation is largely in line with EU directives, but it is very important to improve law enforcement. Some important AMLL provisions are still not fully developed (register of beneficiary owners, list of politically exposed persons, etc). Adoption of a bylaw concerning electronic identification of persons, which will regulate the opening of remote accounts, submitted electronically of all data is still pending.

The register of beneficial owners, as described in the 4th Directive, has become part of Montenegrin AMLL. Harmonization with amendments, brought by Directive 2018/843 are not yet achieved, especially when it comes to access to beneficiary owners register.

Montenegrin law allows direct access to the register only for FIUs in the field of prevention and detection of money laundering and terrorist financing and law enforcers in order to implement measures to establish and verify the identity of the client. Other legal and natural persons must prove their legal interest in accessing this database of beneficial owners. The fee for access to the database exist and its amount is subject to a decision of the Government. This is not in accordance with the 5th Directive that envisage free access to basic data from the register to all interested parties.

[155] The Law on Prevention of Money Laundering and Terrorism Financing (Official Gazete no. 014/07, 21.12.2007; 004/08 17.01.2008; 014/12, 07.03.2012; 033/14, 04.08.2014)

[156] The Law on Prevention of Money Laundering and Terrorist Financing (Official Gazete no. 033/14 from 04.08.2014, 044/18 from 06.07.2018, 073/19 from 27.12.2019)

While under 5th Directive, Member States ensure that the information kept in the central register is adequate, accurate and up-to-date, and establish control mechanisms and ensure that any breaches are subject to effective, proportionate and appropriate measures or sanctions, Montengrin AMLL do not have similar provisions. The Tax administration is the administrator of the central register of beneficial owners, but it is not obliged to determine the accuracy of the entered data. The responsibility lies on the legal entities that enter the data. Not any control mechanism is legaly defined.

In practice, register is still not established. It is in the final stage of preparation. But many open questions remains not defined. The obligation to register beneficial owners is indeed set out in the current AMLL, but no deadlines are specified for such registration by companies that are already entered in the Central registry of business entities (CRPS). The current provisions can be interpreted as requiring registration for new applicants only. There is no obligation to re-register, nor a deadline by which to match the data. These issues cannot be prescribed by a rulebook because a rulebook cannot be more prescriptive than the law in force.

According to 5th Directive Member States shall establish centralized automated mechanisms, registers of bank accounts, where direct access for FIUs and competent national authorities shall be provided. Also, Directive (EU) 2019/1153 provides for the designation of bodies to have access to the central register of bank accounts, as well as the procedure by which those bodies send information to other bodies. These issues are not regulated by the AMLL in Montenegro, and in practice no direct access mechanizam for FIU is established.

However, in practice a Register of Transaction Accounts has been established, but only for Montenegrin residents. According to information obtained from the CBM, which is responsibile for this register, it is currently in the process of expanding the register database for non-residents' accounts. The content of the Register of Transaction Accounts is defined by the Decision on the content of the Central Register of Transaction Accounts[157]. The data from the register are secret, except for users who are allowed to do so in accordance with the law. In accordance with the relevant legal regulations in the field of law enforcement, the CBM is obliged to submit data on the accounts of natural persons to the Public Enforcement Officers. For other competent authorities[158], CBM shall issue a decision on access to this data, if it is assessed that access to such data represents assistance to competent authorities in law enforcement and by court order[159]. In addition to the above, the data are issued to the owner of these data on the basis of his request with mandatory identification, as well as to the person to whom the data owner has given explicit approval. Data from the CBM register are issued in paper or electronic form, with the possession of a qualified digital certificate for authorized persons for access to data. Each approach is recorded and the CBM has data on all downloaded data. Since the beginning of the service, there have been no reported cases of misuse of personal data, according to information obtained from CBM.

The provisions of Directive (EU) 2019/1153, concerning international cooperation, are not harmonized. Cooperation with Europol is not precisely regulated in the AMLL. Detailed information exchange arrangements defining the use of the SIENA system or Fiu.net are not defined by Law.

The exchange of data between FIUs, as well as the competent authorities, is regulated precisely in the AMLL and is partially harmonized with the solutions from Directive (EU) 2019/1153. The difference is reflected in the fact that the Directive stipulates that in urgent cases information is exchanged immediately, which is not the case in the Law.

---

157 Decision on the content of the Central Register of Transaction Accounts ("Official Gazette of Montenegro", No. 48/14 of 13 November 2014 and No. 32/15 of 26 June 2015).

158 Courts, Police Administration, Tax Administration, notaries, communal police, etc.

159 Article 84, Law on Central banks of Montenegro (Official Gazete no. 040/10 22.07.2010; 046/10, 06.08.2010; 006/13, 31.01.2013; 070/17, 27.10.2017)

By AMLL data obtained following legal procedure, supporting documentation, data on the identification number of each client account, data and documentation on electronic money transfer, documentation on business correspondence and reports are kept for at least 5 years after termination of business, transaction, client entry in the casino and premises where other special games of chance or access to the safe are organized, unless a longer period of storage is prescribed by a special law. FATF recommendations, and 4. The Directive indicates that relevant data should be kept for at least 5 years, with the possibility of extending this period to a maximum of 5 years.

Montenegrin AMLL minimum of 10 years, yet leaves the possibility of legally extending the 10-year period, which is not in line with the Directive.

Also, according to AMLL, the FIU is obliged to keep the data and information from the records kept in accordance with Law for 11 years from the day of their acquisition.

Provisions of the AMLL concerning the definition of politically exposed persons and the monitoring of their business are harmonized with the 4th Directive. But, the register (list) of politically exposed persons, although foreseen in the Law as jurisdiction of Agency for Prevention of Corruption (APC) is not jet established. After interview, the director of the APC showed a great degree of interest, after experts' initiative, to prepare methodology for establishing register and data gathering in following months, in order to be put into operation. The issue of collecting and processing personal data on these persons is not sufficiently regulated by the relevant institutions. Given that the register has not been established, it is not possible to determine with certainty how much personal data is protected during processing and exchange within institutions.

When it comes to national risk assessment, AMLL, unlike 4$^{th}$ Directive, do not contain provisions for revising the risk assessment. The national assessment is made in a five-year period, and the law does not provide mechanisms for risk changes that are possible in that period.

The penal provisions of the AMLL are not fully in line with the 4th Directive. Full compliance will be achieved through adoption penal provisions prescribed in accordance with the Law on Misdemeanors[160] which prescribes the maximum fine for committed offenses. According to the Directive, the amount of fines is significantly higher than the maximum set in the Law on Misdemeanors and AMLL and amounts to EUR 5,000,000.

[160] Law on Misdemeanors ("Official Gazette of Montenegro", No. 1/11, 39/11, 32/14, 51/17)

# VI. DATA PROTECTION LEGISLATION

The right to personal data protection is explicitly provided for under article 43 of the Montenegrin Constitution[161], where it is unequivocally guaranteed protection of personal data and forbidden the usage of date outside the purpose for which they were collected.

Based on the above, main important piece of legislation that regulates the protection and processing of the personal data within the territory of Montenegro is the Law on Personal Data Protection (LPDP).[162]

The provisions of the LPDP Law apply to the processing, carried out through automatic means, or through other means, of personal data stored in a filing system, or which are intended to be part of a filing system.

As subjects to such law are considered, *inter alia*, all public controllers of the Montenegro (i.e. including MFIU, Central Bank, etc.).

The public controllers – likewise the private ones – are obliged to process the personal data in accordance with the principles of data processing, i.e. lawfulness and transparency, purpose limitation, data minimization, accuracy (article 10), the criteria on lawful processing, as well as duly and lawfully addressing of the rights of the data subjects, including, but without limitation, their right for access to own personal data, the right to seek the blocking, stopping of data processing and erasure of personal data (article 18), as well as the obligation of the data controllers to inform the data subject on the relevant processing activities (article 21), measures to protect Personal Data (article 24).

The Agency for Personal Data Protection (APDP) is established to perform the tasks of the supervisory body determined by this Law. The Agency is independent in the performance of tasks within its scope. The Agency has the status of a legal entity.

Agency:

1) supervise the implementation of personal data protection in accordance with this Law;

2) decide on requests for protection of rights;

3) give opinions regarding the application of this Law;

4) gives consent in connection with the establishment of personal data collections;

5) give an opinion in case there is a doubt whether a certain set of personal data is considered a collection in terms of this Law;

6) monitor the application of organizational and technical measures for the protection of personal data and propose the improvement of these measures;

7) make proposals and recommendations for improving the protection of personal data;

8) give an opinion on whether a certain way of processing personal data endangers the rights and freedoms of persons;

9) cooperates with the bodies responsible for the supervision of personal data protection in other countries;

[161] Montenegrin Constitution (Official Gazete no.001/07 from 25.10.2007, 038/13 from 02.08.2013)

[162] Law on Personal Data Protection (Official Gazete no. 001/07 from 25.10.2007, 038/13 from 02.08.2013)

10) cooperates with the competent state bodies in the procedure of preparation of regulations related to the protection of personal data;

11) make a proposal for assessing the constitutionality of the law, ie the constitutionality and legality of other regulations and general acts regulating the issues of personal data processing;

12) perform other tasks in accordance with the law governing free access to information and this law.

## VI.1 Legislation development

According to Article 9 of the Constitution, the ratified international treaties and generally accepted rules of international law represent an integral part of the domestic legal order.

In December 2003 State Union of Serbia and Montenegro ratified the European Convention on Human Rights and Fundamental Freedoms ((i.e. including article 8 thereof – Right to respect for private and family life) and its fourteen protocols. The 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, ratified by the State Union of Serbia and Montenegro in 2005.

Following independence, in July 2006 Montenegro submitted a statement of succession to the Council of Europe in relation to all the conventions signed by the Sate Union of Serbia and Montenegro. Montenegro became a member of the Council of Europe in 11st May 2007.

In December 2008, the Data Protection Law is approved. Since then, this instrument has been amended three times. The first amendment was approved in November 2009, the second amendment in August 2012 and the third in April 2017.

The Agency for Personal Data Protection and Free Access to Information was established in accordance with the provisions of the LPDP, as an independent body. Since 2009, the election of the Agency's bodies (Council and Director), the creation of organizational and technical conditions for work, the adoption of bylaws, etc. The Agency is in function of the purpose for which it was established.

New LPDP is being prepared and in the fourth quarter of 2021, the Government is expected to adopt it. Institutions, taxpayers, and the civil sector were very interested in cooperating in drafting the legal text and more than 40 subjects participated in the public consultations, and the report from the public consultations is 280 pages long[163].

## VI.2 Level of approximation with *aquis communitaire*

The harmonization of LPDP with relevant Directives and EU standards of personal data protection is on lower level, which has stimulated the need to draft a new legal text during the preparation of which special attention is paid to approximation.

The interlocutors believe that in the field of personal data protection, both Ministry of Interior and the APDP are committed to the harmonization of national legislation with the EU. On the other hand, when it comes to efficiency and supervision, evaluations are not equally positive. In most countries, there is a department in the Ministry of Justice that deals with personal data protection. In Montenegro it is the Ministry of Internal Affairs. LPDP was amended in accordance with the 2015 Regulation.

The LPDP is fully approximated with Directive 95/46/EC. Furthermore, LPDP is mainly approximated

[163] Information from the interview, Data Protection Unit, Ministry of Interior

with Regulation 2016/679 of the European Parliament and the Council, as well as Directive 2016/680. Data processing of minors and Informing respondents about data processing in domestic legislation is regulated less precisely than in the Regulation and the Directive, which may lead to a reduced scope of the rights of these persons.

Namely, there is only one paragraph in the article in the Montenegrin LPDP that regulates the processing of data of minors, which states that the data will be processed "in the best interest of the minor and in accordance with the law." In contrast, the Regulation states that data processing is legal for a person aged 16 and over. It is also stated that it is legal for a person under the age of 16 if the consent was given by the "holder of parental responsibility over the child".

Also, unlike the LPDP, the Regulation stipulates that the respondent will be informed of the contact details of the data protection officer and the period in which the data will be stored. In addition, the Regulation specifies more precisely the exceptions to the obligation to inform respondents.

The law provides for similar definitions of general terms as Regulation (EU) 2016/679. The most important terms (personal data, processing, processing manager, processor) are generally similarly defined. However, the Regulation defines more terms (26) than the Law (9). Some of the terms defined in the Regulation, which are not in the Law, are important and should be defined (eg personal data breach). Also, consent is more precisely defined in the Regulation than in the Law.

The LPDP is not harmonized with the Directive (EU) 2019/1153 when it comes to the statistic provisions. Directive obliges the state to keep statistics on the amount of information that national authorities managing central registers of bank accounts send to the competent authorities through an automatic mechanism (quantity of requests, time required for response, costs of human or IT resources).

The LPDP uses the term "special category of data" for the processing of sensitive personal data. It is precisely regulated when this data can be processed and that unauthorized access to data is prevented. However, unlike the Directive (EU) 2019/1153, it is not emphasized that "only specially trained staff can access this data" and that "it can process it under the guidance of a data protection officer.

Measures for the protection of personal data from the LPDP are partially harmonized with Directive 2016/680. Not all forms of data security protection from the Directive have been transposed into the Act (lack of data carrier control, communication control, transmission control).

# VII. AML LEGISLATION VIS-À-VIS DATA PROTECTION

For purpose of assessing the extent to which the provisions of the AML Legislation account to the principles and criteria on the lawfulness of processing of personal data, it should be differed between the formal normative situation (i.e. systematic compliance of the provisions of each legislation) and the institutional behavior of the public bodies/authorities, which process personal data in the ambit of AML Law, vis-à-vis the Data Protection Law.

The provisions of Law on PDP itself are largely incorporated into the AML law, implemented by FIU. It prescribes which records are kept, in what way and by which persons the data are used. They have their own completely closed information system which is under full control and positively evaluated by international entities. Data on logging, the amount of information used and the purpose are carefully monitored, both for the internal information system and for access to other databases.

Based on the constitutional approach that the processing of personal data (i.e. including the eventual obligation of data subjects to disclose them) is subject to (specific) law provisions or to the (informed) consent of the data subject, there is no reasonable room for alleging that the provisions of AML Law – in principle – are not in compliance with those of Data Protection Law.

On the other hand, despite the above (negative) normative compliance assumption between such laws, there have been several cases when the *de facto* requirements that public entities (i.e. Tax Administration) have imposed on the data subjects, in virtue of an extended interpretation of the AML Law, have violated the provisions of the Data Protection Law. In this view, it is to be mentioned, for example, the practice of Tax Administration to require information on both revenues and outcomes in several cases, although such requirement is necessary only for revenues in order to calculate tax liability. It is relevant to this topic as it present misunderstanding of data protection by Tax administration in certain cases.

As mentioned above, the processing of personal data is to be based on (specific) law provisions or consent of the data subjects.

In the opinion of the Agency for PDP, the amount of personal data that is collected is often higher than the needs, which data are needed to achieve the purpose. Personal data protection measures must exist, and every personal data controller must take strict care to ensure these measures and prevent misuse.

All document collection managers and processors must ensure that users of personal data, the data being processed, the legal basis, logins to the system and other data are registered in the information systems.

The above example shows the difference between the normative regulation of AML Law and the institutional behavior of AML enforcing bodies. Controlling mechanisms are not fully developed as Agency for Personal Data Protection should act more proactively.

In a situation where the relevant registers provided by law are not functional and established, and when interoperability is not at a satisfactory level, it is not easy to draw a conclusion about the degree of protection of personal data in the field of anti-money laundering. The general conclusion is that more attention needs to be paid to this issue. in addition to good legal solutions, law enforcement needs to be improved.

It is important that a new law is being drafted that will prescribe additional records kept by the FIU, as well as records related to customs, bank records and safes. The provisions of the AML law concerning the register of beneficial owners will be improved in terms of setting a deadline for the registration of existing legal entities, but also the liberalization of persons who have access to basic data.

When it comes to the new PDP law, it is under the authority of the Ministry of Interior, and the Agency participates in its preparation. It is planned to be done in the IV quarter.

Provisions of the 5th Directive will be part of the new AML law, and according to directive 679/2016, work is underway to harmonize the law on PDP.

Alignment with the GDPR will be part of PDP law, and the Police Directives will be part of the new legal text. This new law also being prepared, in line with Directive 680, which concerns the protection of personal data when it comes to law enforcement authorities. AML law will be harmonized with directives 680 regarding personal data and 1153/2019 on the manner of using financial data.

## VII.1 Institutional approach and aspects

The institutional approach and behavior of AML enforcing authorities is to be analyzed, both, from the monitoring/supporting and supervising perspective of the Data Protection Law.

The general assessment is that more knowledge in this area is needed in all bodies. That is why training on this topic is necessary. One of the stakeholders pointed out that perhaps the Prosecutor's Office should also open a space for one prosecutor who is especially expert in the field of personal data protection.

The system of the collegial body (the Council of the Agency for Personal Data Protection) was criticized by our interlocutors, who assessed that it was not good, but that one person should be at the top.

The new Law protects the level of personal data protection to a higher level, complicates the work of data processing, and raises technology to the highest level. Challenges in the future implementation of the new Law are already visible in terms of technical readiness of bodies and taxpayers, the establishment of modern IT solutions and budget allocations for this purpose.

Currently in Montenegro, the situation is such that the degree of personal data protection depends on the management of the institution and the willingness to apply the law. The key person for ensuring implementation is the manager and his decisions, which means that in essence the awareness of personal data protection within the institution depends on the will of the superior.

The work of the Special State Prosecutor's Office, which is responsible for prosecuting money laundering offenses, is regulated by procedural laws. Data protection to which prosecutors have access is ensured, reconnaissance and investigations are classified to varying degrees. Until the indictment is filed, all data available to the prosecution from other entities are protected.

When certain data from other state bodies are used, all prosecutors and associates have licenses on the basis of which they access certain databases. Labels range from internally to top secret, and in their work they are guided by it. All in accordance with the Code of Criminal Procedure, other regulations.

Interoperability is not always established. Direct access to databases of Central Bank (CB) and Ministry of Interior is established. Licensed employees of SPO have direct access to databases with login recordings on time, date and scope of information obtained. But problem remains communication with other institutions which is conducted in "paper form". When it comes to AML investigations, not only access to data of other employees is problem, but as well time needed for reply to be secured by relevant institutions.

Also, the problem is the situation that the response to the request of the prosecution is incomplete and that a new round of communication with certain bodies must pass in order to complete the request.

This procedure slows down work of SPO, and for that reason they constantly advocate and insist on connected and accessible databases for all relevant institutions, so that they can obtain the appropriate information at the time of interest. The SPO emphasizes that minutes are crucial in money laundering investigations and that this way of working is not in favor of the efficiency of the investigation.

In the manner of PDP regulations, having direct approach to databases would also secure that personal data be better protected.

On May 7, an Agreement in the field of crime prevention was signed to improve cooperation between the Ministry of Interior, the Police Administration, the FIU, the Ministry of Finance, the Ministry of Justice, the Supreme Court, the Supreme State Prosecutor's Office, the Judicial Council, and the Central Bank. It replaced the agreement from 2017, which was partially respected, ie it was fully respected only by the FIU. Agency for Prevention of Corruption is not part of this Agreement and in following period, according to their proposal, it would be useful to be included. This is very important because RAI recently initiated regional network for exchange of real estate data, which is run by APC.

Automatic data exchange takes place between all institutions. This includes the revenue administration (taxes, customs and games of chance) and data from the real estate administration. The agreement contains precisely stated information that is exchanged and in what way. Also, the agreement contains provisions on mandatory protection of personal data during data processing and exchange.

FIU used to exchange data according to old agreement and still has access to many databases, including databases of police and Ministry of interior, Ministry of Justice, tax administration, Judicial Council, CB. They insist on obtaining access to real estate register, including registration history for a property.

The provisions of Law on PDP itself are largely incorporated into the AML law, implemented by FIU. It prescribes which records are kept, in what way and by which persons the data are used. They have their own completely closed information system which is under full control and positively evaluated by international entities. Data on logging, the amount of information used and the purpose are carefully monitored, both for the internal information system and for access to other databases.

In the opinion of the Agency for PDP, the amount of personal data that is collected is often higher than the needs, which data are needed to achieve the purpose. Personal data protection measures must exist, and every personal data controller must take strict care to ensure these measures and prevent misuse.

All document collection managers and processors must ensure that users of personal data, the data being processed, the legal basis, logins to the system and other data are registered in the information systems.

Institutions in Montenegro often ignore the fact and legal obligation of all bodies to submit to the Agency the registration of records of personal data they have used. The Agency is not interested in a list, scope of data or purpose, but is submitted according to a special form on which legal basis and which personal data the institution collects.

The processing of personal data related to money laundering was not the subject of complaints from citizens for violations of the right to privacy or personal rights before the Montenegrin branches.

In general protection of personal data is not in focus, and one of the priorities of state administration bodies. The Agency for PDP, as a supervisory body, is quite dissatisfied with the attitude towards the protection of personal data by institutions and people who process data.

The Montenegrin Financial Intelligence Unit (MFIU) uses data from other bodies intensively, in which case it complies with the applicable law on personal Data Protection.

On May 7, an Agreement in the field of crime prevention was signed to improve cooperation between the Ministry of Interior, the Police Administration, the FIU, the Ministry of Finance, the Ministry of Justice, the Supreme Court, the Supreme State Prosecutor's Office, the Judicial Council, and the Central Bank. It is based on inter-institutional cooperation for automatic exchange of data. It replaced the agreement from 2017, which was partially respected, ie it was fully respected only by the FIU.

An efficient web service has been established, which guarantees data protection, access restrictions, logging records and user identification. It also records who, based on which act and why accesses the data. So far, no reports of abuse of the data exchange system have been recorded.

Yet, the exchange of data does not function in relation to the MFIU - State Prosecutor's Office. The problem is in the compatibility of the prosecution's IT system.

Cooperation between the MFIU and the Central Bank (CB) has been going on since 2014, and in 2019, the CB and the MFIU signed a bilateral cooperation agreement. The agreement clearly prescribes obligations and responsibilities. The cooperation was assessed as excellent, from joint work on amendments to the Law, weekly communication, agreeing on joint actions, joint trainings. Cooperation between the MFIU and the CB is very important due to the 5$^{th}$ Directive. It includes the data necessary for the MFIU, primarily the Register of Bank Accounts and Safes. The registry will be kept by the CB, but its main law is the Prevention of Money Laundering and Terrorist Financing. The 5th Directive stipulates that there is no anonymization of accounts and safes and the MNE legal system is in compliance with the Directive.

Access to data and data exchange within the country does not work between the FIU and the real estate administration, but it is being worked on. For now, the FIU uses the publicly available database or addresses a request.

## VII.2 Material approach and aspects

There are several aspects of personal data protection legislation that should be taken into account when determining the material/normative approach that will be pursued by AML legislation.

At first, there is always the need to have the provisions of both legislations fully aligned with one another, serving this way to the legal certainty principle that allows all stakeholders (i.e. controllers and data subjects) to predict their institutional and personal behavior vis-à-vis Data Protection Law, when, simultaneously, addressing the requirements of AML Law.

Secondly, clear and very well-reasoned and accurately outlined levels of access to the personal data should be granted to third parties, who are entitled thereto by letter of law. The levels of access should be clearly determined, both, in relation to internal staff and third parties outside the organization, so to keep track of the processing activities and accessing persons.

## VII.3 Conclusions

The general conclusion is that institutions are actively working to improve the system when it comes to AML/DP, but these activities, in the context of 5$^{th}$ Directive especially, can only be considered initial. In addition, very rapid changes in this area, at the international level, make it difficult to strike a balance between the legal framework and practice. Some systems work well in practice, although they are not yet shaped by the legal framework, and this primarily refers to the work of FIUs, their

communication channels and the way they work. However, some legally recognized institutes have not yet been established in practice (register of beneficial owners and PEL register).

The fact that concrete work is underway to improve the AML/DP legislation, with a precise implementation of the provisions of the Directives, indicates that full compliance, but also the coincidence of practice with the legislative framework can be expected only in the coming period.

Institutional readiness and the will to protect personal data in money laundering investigations exist. Institutions follow what is required by the secrecy of investigations or strict international rules, while consulting the PDP Agency for concerns. In the opinion of the Agency as a supervisory body in this area, human resources in terms of the applicable law exist, although the protection of personal data is still not a key priority in the work of institutions. However, bearing in mind that the current law is still in the phase of change, following the GDPR and EU directives, continuous training at all levels has already crystallized as a need.

Another problem is that full interoperability in data exchange has not yet been established and that much of the work is still done "on paper", which reduces data security. However, violations and abuses are very difficult to prove in practice, while institutions point out that there was no report or misuse of personal data.

The Law on Prevention of Money Laundering and Terrorism Financing (LPMLTF) is almost completely harmonized with the Directive 2015/849, the part that is not harmonized concerns the misdemeanor responsibility and the amount of fines, which are more closely prescribed by the law on misdemeanor proceedings. Harmonization with amendments to Directive 2015/849 brought by Directive 2018/843 are not full achieved, especially when it comes to access to beneficiary owners register.

Montenegro started incorporating the newly introduced standards only a year and a half after the Directive 2019/1153 entered into force, by establishing a working group to draft a new Law. In this moment Law is not harmonized in provisions that regulates establishment of central register of bank accounts, cooperation with Europol, etc.

In the field of data protection, The Data Protection Law (LPDP) is fully approximated with Directive 95/46/EC, it is mainly approximated with Regulation 2016/679 of the European Parliament and the Council, as well as Directive 2016/680. According to our interlocutors, the protection of personal data still depends on the will of the managers of the institution and their awareness of the importance of protection. In preparing a new law that should bring greater harmonization with aquis communitaire, the institutions express concern about the readiness of the system to implement this modern law.

AMLL was last amended in 2019 and is fully in line with the 4$^{th}$ Directive in the field of prevention of money laundering. However, the law is not in line with the 5$^{th}$ Directive and the government plan is to adopt a new Law on the Prevention of Money Laundering because the amendments will be in more than 50% of the content of the law currently in force. These amendments would incorporate the 5th Directive. The Government planned to complete the drafting of a new law in the third quarter of 2021.

After conducting interviews, the interlocutor assessed that cooperation and data exchange work well in practice both within the country and internationally. An agreement on inter-institutional cooperation (internal act) for automatic exchange of data signed between the Ministry of Interior, the Ministry of Justice (which includes criminal records), the Ministry of Finance (which includes the Tax Administration and the Customs Administration), the Supreme Court and the State Prosecutor's Office is a very important and used in practice for cooperation of state bodies that have jurisdiction in Anti-Money Laundering issues. Access to data and data exchange within the country does not work between the FIU and the real estate administration yet. With regard to legal provision on

international cooperation and data exchange, the AMLL is not harmonized with the provisions of the 5th Directive in the field of cooperation with Europol, on the provision of bank account information to Europol, the exchange of information between Europol and FIUs and the detailed information exchange arrangements.

The Law on Personal Data Protection (LPDP) is harmonized with Regulation 2016/679 of the European Parliament and the Council, as well as Directive 2016/680. However, the question remains as to how successfully the Law is applied in practice. Although the 5th Directive in the field of prevention of Money Laundering is partly related to Data Protection, the Government intends to implement the 5th Directive not through amendments to the Law on Personal Data Protection, but through the new AMLL.

It is very important to adopt a bylaw concerning electronic identification of persons. This issue has its starting point in the Law on electronic signature and electronic identification. The implementation is supervised by the Ministry of Public Administration, Digital Society and the Media. The use of this data, interoperability and the use of the electronic identification register are closely related to the protection of personal data, for that reason, it is necessary to link this process in terms of parallel development of software solutions and control. Compliance of this area with the 5th Directive, it is not possible to assess in the current situation, when not all legal mechanisms are established and functional.

There is a problem with the implementation of AML Law due to institutional capacities. The general assessment is that more knowledge in this area is needed in all bodies. Challenges in the future implementation of after the amendments to the Law are already visible in terms of technical readiness of bodies and taxpayers, the establishment of modern IT solutions and budget allocations for this purpose.

The register of beneficial owners, which according to AMLL is responsibility of Tax Administration, is in final stage of preparation. Yet, legal provisions that regulate access to register and maintenance are not in accordance with 5th Directive. The reliability of the data is not guaranteed, nor the possibility of free access for the general public and interested parties. The law do not regulate the issue of registration of existing legal entities, deadlines and procedure.

The register of politically exposed persons, which is part of AMLL is not yet established, for that reason the methodology of data collection from banks and other legal entities, the method of data processing and the degree of personal data protection cannot be assessed. This register is responsibility of APC, which is also responsible for keeping the register of public officials.

Montenegrin authorities have established a comprehensive system and are making significant efforts to provide a wide range of various forms of international cooperation, including through mutual legal assistance, international police cooperation and FIU – to – FIU cooperation. However, it is still not fully clear how data and information obtained through international cooperation channels are used effectively in the criminal prosecution of these criminal offences in Montenegro.

It seems that the cooperation is most developed at the FIU-to-FIU level, as well as at the level of operational police cooperation, and also because the secrecy of investigations does not allow for the presentation of such data at MLA level. However, the number of cases and judgments in the field of money laundering and especially terrorism financing, is so small that it cannot have a deterrent character and effect, not prove the effectiveness of the cross-border cooperation to a larger extent, although that does not necessarily exclude the existence of comprehensive data exchange at the operational level.

When it comes to international cooperation and data exchange, adequate level of data protection is met by the adherence to the relevant points of the Principles of Egmont Group, EU data protection standards and relevant national legislation.

# VIII. RECOMMENDATIONS

- The Law on Prevention of Money Laundering and Terrorist Financing (Anti-Money Laundering-AMLL) should be harmonized with 5th Directive.
- Data processing of minors and Informing respondents about data processing in domestic legislation is regulated should be as precise as the Regulation 2016/679 and the Directive 2016/680.
- Interoperability needs to be established among relevant institutions to decrease risk of misuse of personal data in institutional exchange.
- Direct data exchange between the FIU and the Prosecutor's Office should be established, through the establishment of a compatible IT system that will enable interoperability.
- Institutional capacities should be strengthened, in terms of strengthening information literacy and the use of modern software and IT solutions.
- Special attention must be paid to establishing a register of beneficial owners in accordance with 5th Directive this issue requires a change in legal provisions, bylaws and practical implementation. Here it is especially important to regulate access to the register in accordance with the Directive, but also to resolve issues of re-registration and procedures for existing entities.
- Register of political exposed persons should be established, enabling direct access to relevant institutions, instead of list defined in current AMLL
- Register of political exposed persons and beneficial ownership register should be formed following a methodology of data collection and processing that will guarantee the security of personal data and prevent misuse.
- Bylaws concerning electronic identification of persons, which will regulate the opening of remote accounts, submitted electronically of all data, should be adopted and harmonized with 5th Directive.
- It is necessary to improve the legislative framework in the field of games of chance, for which there was no political will in the previous period, having in mind the connection of this area with money laundering, but also the processing of personal data of persons who are users of games of chance.

# CROSS BORDER COOPERATION IN AML/CTF ISSUES

Policy analysis for Montenegro

**Podgorica, May 2021**

# INTRODUCTION

Tackling cross-border money laundering and terrorism financing, by detecting and deterring illicit transactions, has become an overriding issue in recent years. Lessons learnt so far in dealing with globalizing criminal industry outlined a need for stronger governance and risk management, as well as for enhanced information flows among financial regulators, judiciary and law enforcement. Several high-profile cases with cross-border elements, prosecuted in Montenegro, also call upon stronger AML/CTF supervisory architecture and better legislative and institutional frameworks and capabilities for addressing connections among money laundering, organized crime and dark economy, especially those relating to crypto currencies.

The Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) and FATF, Paris-based standard-setter both provide extensive AML/CTF guidance and sector assessments, however, problems in information exchange continue to constrain cross-border supervision and financial integrity oversight. In order to provide for a structured, collaborative and coordinated response to AML/CTF, the EU has developed bloc-wide systems, including Schengen Information System and Europol, and produced a series of directives, starting from 1st AML Directive adopted in 1990.

The 5th anti-money laundering Directive (Directive (EU) 2018/843) on 19 June 2018, inter alia, set up central bank account registries or retrieval systems in Member States, with a view to allow Financial Intelligence Units (FIUs) access to broad information for carrying out their tasks. The Directive also covers crypto currencies, custodian wallet providers, estate agents, rental intermediaries and art dealers. The also Directive and the EU data protection framework allow for full compatibility of exchange of information amongst FIUs and third countries.

The Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laid down rules for the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA.

The new Directive, dubbed as 6AMLD, recognizes 22 predicate offense underpinning money laundering and extends criminal liability to legal persons, while introducing dual criminality standard and tools to determine which Member State will have a jurisdiction. The Directive requires member states to improve international cooperation in investigating and prosecuting cross-border money laundering cases. Under the new rules, one member state can act as the 'hub' of legal actions relating to money laundering cases.

According to this Directive, whose practical implementation by obligated entities within Member States is expected by 3 June 2021, Europol provides support to cross-border investigations by Member States' into the money laundering activities of transnational criminal organizations. According to this regulation, Europol national units are the liaison bodies between Europol and the Member States' authorities, competent for criminal investigations.

On 24 July 2019, the European Commission adopted a Communication entitled "Towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework. " On 7 May 2020, the European Commission adopted a comprehensive action plan for Union's AML/CTF policy which is built on six pillars, including on cross-border cooperation.

Recently, the European Banking Authority, an EU agency, issued guidelines on cooperation and information exchange for AML CFT supervisory purposes which outline and clarify the practical modalities of cooperation and information exchange between AML/CFT competent authorities, domestically and on a cross-border basis. These Guidelines are developed to foster a common

approach to AML/CFT within the EU, which is also expected to impact on the approach of the EU acceding countries in dealing with these crime phenomena.

As the EU declared AML/CTF one of its priorities until 2024, much of the current debate with Members States focuses on creating a single EU rule book as well as a central EU AML agency.

Adopting, implementing, and enforcing international standards against money laundering and financing of terrorism, in particular 40 recommendations and 9 special recommendations on terrorist financing of FAFT are considered one of the key priorities for Montenegro on its path towards the EU.

The aim of this paper is to examine the available national arrangements for cross-border cooperation in AML/CTF cases, including through mutual legal assistance, international police cooperation or Egmont Group's Charter, with the aim to contribute to an effective and efficient national AML/CTF framework and to make up-to-date policy recommendations on the subject.

# OVERALL BASELINE OF AML/CTF SITUATION IN MONTENEGRO

Montenegro has been long affected by multiple organized crime threats. Its geographic location has made it an attractive target for money laundering, as it is placed at the "Balkan route", i.e. the main corridor for smuggling illicit goods from Middle East and Turkey to Western Europe. Factors that facilitate Montenegro's vulnerability to money laundering, in addition to the existence of significant black market for smuggled items, are the use of cash for large commercial transactions and a lack of monetary controls over currency use, as Montenegro uses the euro, but is not a Eurozone member country.

Additional factors include corruption, insufficient capacity to conduct proactive financial investigations, weak collaboration among government agencies, and a judicial system perceived as susceptible to political influence.

As a candidate country on its path to join the European Union (EU), Montenegro has invested important efforts in EU accession negotiations, particularly under Chapters 23 and 24. In order to counter organized crime & corruption and tackle AML/CTF, Montenegrin institutions worked to establishing an efficient and reliable AML/CTF regime.

Montenegro ratified international conventions on the suppression of organized crime and terrorism, UN Palermo and Mérida Conventions, Council of Europe Convention for the Suppression of the Financing of Terrorism and the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

The 2014 national legal framework governing AML/CTF was upgraded and money laundering offence broadly put in line with the Vienna and Palermo Convention. The financing of terrorism offence is being applied to financing of terrorist organizations and individual terrorists without any link to the commission of a specific terrorist act. AML/CTF is recognized by the national 2018/2019 SOCTA (serious and organized crime threat assessment).

The national intelligence model of prioritization, management and allocation of tasks in the field of countering serious and organized crime, including money laundering and terrorism financing, was developed in 2015. The national Strategy for the Fight against Corruption and Organized Crime 2010-2014 expired in 2015, and was replaced with the Operative Document for the Fight against Corruption in January 2016. Although that Document expired in 2018, the new Strategy for 2019 – 2022 was not adopted yet, despite plans to do so in 2018.

The second National Risk Assessment (NRA) was adopted by the Government in October 2020 (the 1st one dates back to 2015), as well as MONEYVAL Work Plan for the period 2020-2022.

The Administration for the Prevention of Money Laundering was first established in 2003, and reorganized in 2007, having covered the terrorism financing as well. In 2012, the Administration got the status of an independent administrative-type FIU, with a legal basis for receiving, analyzing and disseminating of disclosures of suspicious transaction reports (STRs). In December 2018, the Police Directorate was changed into a separate entity from the Ministry of Interior. At the same time, the Administration for the Prevention of Money Laundering and Terrorism Financing ceased to exist under its previous legal form. A Sector for Prevention of Money Laundering and Financing Terrorism was established within the Police Directorate, serving as Montenegrin FIU. According to the new Rulebook on the internal organization and systematization of the Police Directorate, which was adopted in March 2021, it was renamed to the Financial Intelligence Sector.

After the change of the organizational status if FIU in 2018, and given the fact that Egmont Group membership is linked to a particular unit (and may not automatically move to another body in case

of changes to the FIU system in a given jurisdiction), Montenegro was no longer a member of the Egmont Group that it used to be since 2005. The Montenegrin FIU re-applied for Egmont Membership in December 2019, supported by FIU Albania and FIU Azerbaijan. As per the decision of the Chiefs of Financial Intelligence Units made on 4 November 2020, FIU Montenegro is again a member of the world's largest network of financial intelligence units.[164]

**Montenegro is bound by international obligations on the basis of the membership in FATF[165] and MONEYVAL, as well as FIU's participation in Egmont Group, since 2005. Also,** since 2010, Montenegro also has an **observer status in EAG** (Euro-Asian Anti-Money Laundering Group and Terrorist Financing).

[164] P.4 of the Annual Report of FIU for 2020, published in March 2021.

[165] **Montenegro is not on the FATF List of Countries, which have strategic AML deficiencies.**

# OVERVIEW OF AML/CTF LEGISLATION AND INSTITUTIONAL INFRASTRUCTURE

In recent years, Montenegro made important changes to its national legislation concerning AML/CTF, primarily to the Law on Prevention of Money Laundering and Terrorism Financing (LPMLTF), the Criminal Code and legislation concerning the work of the Central Bank, insurance companies and others. Montenegro also adopted its first Action Plan on the Implementation of UNSCR 1373 (2001) in 2017. The Law on International Restrictive Measures was adopted in 2015 and amended in 2017, to regulate procedures for freezing of terrorist funds or other assets of designated persons listed under UNSCR 1267 and 1373. The Law is mostly applied to the situations when an international organization, such as the United Nations or the European Union, introduces a restrictive measure against a named individual, state or entity.

The Law on the Prevention of Money Laundering and Terrorism Financing Montenegro (LPMLTF[166]) governs the establishment, content, bases of recording and manner of keeping the register of beneficial owners of legal entities and other entities registered in Montenegro. In follow up of the 4th round mutual evaluation report of MONEYVAL which took place in April 2015,[167] amendments were made to LPMLTF, notably with respect to the requirements of the 5th AMLD. The last amendments were adopted by the Montenegrin Parliament on 17 December 2019. The amended LPMLTF regulates the competencies, powers, affairs and organization of the Police-based FIU, including the Protection of data and information kept by it. It also establishes conditions for creating functional PEP lists.

According to MONEYVAL, Montenegro has also made significant progress in addressing many of the identified deficiencies under R.1 (criminalization of money laundering), 3 (confiscation measures), 5 (customer due diligence), 13/SR.IV (suspicious transaction reporting), 23 (supervision), 40/SR.V (international cooperation), SR.I (international conventions on terrorism financing), SR.II (criminalization of terrorism financing) and SR.III (freezing of terrorist funds), which has brought the level of compliance with these recommendations to "largely compliant". Due to afore-mentioned changes at the legislative level, in May 2020, MONEYVAL formally removed Montenegro from the fourth round's regular follow-up process,[168] considering that the country had taken sufficient steps to remedy deficiencies that had been identified in 2015. [169]

However, certain elements of the legislation are still not fully in line with the EU directives. The current register of beneficial ownership, including the one that exists within the Tax Administration as well as the Central Register of Business Entities (CRPS) are not fully compliant with the requirements of the 5th AMLD. There are still no sanctions for a failure to submit requested ownership data. Hence, the identification of the real owners of private companies and tracing of their financial transactions is expected to remain challenging.

Other areas of concern remain related to implementation of preventive measures and to FATF recommendations, in particular to the practical implementation of FT Convention requirements (as the case law in this area practically does not exist so far), and of **Recommendation 23 (Regulation**

166 „Official Gazette of Montenegro" No. 033/14, 044/18 and 073/19

167 The on-site visit to Montenegro took place from 3 to 8 March 2014. MONEYVAL adopted the fourth round MER of Montenegro at its 47th plenary meeting (14 - 17 April 2015). As a result of the fourth round evaluation process, Montenegro was rated partially compliant (PC) on 24 Recommendations1 and non-compliant (NC) on 4 recommendations, including on several core2 and key3 recommendations. Following the adoption of the 4th round mutual evaluation report ("MER") at MONEYVAL's 47th Plenary in April 2015, Montenegro was placed under the enhanced follow-up procedure pursuant to Rule 13 of the revised Rules of Procedure, and Step 1 of the Compliance Enhancing Procedures ("CEPs") applied.

168 Montenegro submitted its first regular follow-up report, after named FIU organizational changes, at the 58th Plenary meeting held in July 2019. The Secretariat concluded that it could not assess at that stage whether Montenegro fulfilled the criteria for removal from the 4th round follow-up process (as set out in Rule 13, paragraph 4 of the 4th Round rules of procedure), given that the country's AML/CFT system was undergoing changes.

169 https://www.coe.int/en/web/moneyval/-/montenegro-exits-moneyval-s-fourth-round-regular-follow-up-procedure

**and Supervision of Financial Institutions)**, where low number of AML/CFT infringements and low efficiency of on-site inspections has remained.[170] Also, FIU is not specifically stipulated as a supervisory authority for financial leasing companies according to the new LPMLTF.

In relation to **Recommendation 40 (Other Forms of Cooperation) and SR.V (International Cooperation)**, most deficiencies have been addressed since 2015, bringing the level of compliance with R.40 to „largely compliant"(LC). Montenegro is urged to address the outstanding deficiencies outlined in R.40 before the 5th round mutual evaluation, including with respect to effective exchange of data related to predicate offences (that LPMTF provides for) and the authorization of the auditors and experts to exercise direct control which should be granted not only to EU Member State countries, but also to third countries.[171]

As it comes to FIU, it is organized as per police-based financial intelligence unit as of 2019 effectively. FIU is independent in exercising its powers and decision-making related to: (i) the reception, gathering, keeping, analyzing and delivering of data, notifications, information and documentation; and (ii) sharing of strategic and operational analysis of suspicious transactions to the competent authorities and foreign FIUs.

The head of the FIU is appointed by the Government, following public competition, upon the proposal of the director of the administrative authority competent for police affairs. Regarding FIU's budget, funds are allocated to it by the budget of the administrative authority competent for police affairs, and independently disposed of by the head of the FIU, in accordance with instructions given by the director of the administrative authority competent for police affairs.

FIU can request information from reporting entities, regardless of temporary freezing of a transaction and monitoring the client, etc. Additionally, suspicious transactions are reported to FIU. Authorities that are in charge of monitoring compliance with the key AML/CTF obligations include also the Central Bank of Montenegro, the Insurance agency, the National Customs Agency, the Montenegrin post and the relevant inspectorate.

FIU has direct access to the electronic database of beneficial ownership of legal persons. Beneficial ownership information also serves to enhance public scrutiny and contribute to preventing the misuse of legal entities for money laundering and terrorist financing purposes. Access to data on the beneficial owner of trusts is also granted to FIU. Only FIU has a direct /automatic access to the Central Bank's databases, as provided under the relevant EU acquis.[172]

Also, FIU has electronic access to Customs authority data on cross-border transportation of cash, bearer securities and precious metals with a value or amount of EUR 10,000 or more, that were not declared.

FIU has 30 positions, including 17 dealing directly with cases (increased from 10 in the previous FIU). The existing Case Management System (CMS) used by FIU allows operators to analyze information quickly; however, implementation of additional tools like a single search feature across available national police databases is needed. Once a year, FIU publishes a report that includes statistical data, trends and typologies in ML/FT, and especially data related to the number of STRs sent to the FIU.

Formation of cases (analysis of persons and transactions) can be initiated by foreign financially intelligence services. After receiving the request, in accordance with the procedure, access is made to collect the necessary data and then analyzed them by the FIU officers.

Regarding the protection of information kept by the FIU, LPMLTF stipulates that the FIU shall, in

[170] Revised Exit Follow up report submitted to MONEYVAL, May 2020, https://rm.coe.int/moneyval-2019-31rev-mgr-4thfollowuprep/16809e6485

[171] *Ibid*, please see the text referring to R40.

[172] European Commission, Montenegro 2020 Report, page 47, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/montenegro_report_2020.pdf

the aim of protection of data and information kept in accordance with the Law, provide technical conditions for the protection of those data and information. Also, access to such data and information is solely provided to FIU employees.

Although FIU achieved certain results in confiscating criminal proceeds, gaps still remain in terms of full compliance with international conventions and FATF.[173] **The European Commission, in its reports on Montenegro, urged for intensifying international cooperation efforts, in line with FATF recommendations**. The Commission also called for a review the legal & operational approach towards financial investigations, money laundering, asset recovery, as well as for an integrated approach between all relevant bodies in order to build a convincing track record in this area. [174]

[173] **Ten preliminary investigations and seven investigations into money-laundering were conducted in 2019, regarding 122 entities, including one case of a value of EUR 25 million. There were two final convictions for money laundering in 2019, both achieved through plea agreements. In 2020, criminal charges against 34 persons were submitted, while 26 charges derived from 2019. Out of 60 criminal charges, Special Prosecution Office (SPO) raised 4 indictments, and issued 19 orders for investigation: Annual Report of the SPO for 2020,page 27 - 30, https://sudovi.me/static//spdt/doc/Izvjestaj_o_radu_SDT-a_za_2020.godinu.pdf**

[174] Montenegro 2020 Report, https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/montenegro_report_2020.pdf

# MODALITIES OF CROSS-BORDER COOPERATION IN AML/CTF CASES

Due to the transnational nature of money laundering and terrorism, the cross-border cooperation is of paramount importance. While certain solutions may be tailored to meet specific country needs, cross country operational efficiency has appeared as far more challenging. FATF recommendations 37 and 38, in particular, call for mutual legal assistance as well as the expeditious actions to be taken in response to requests made by foreign countries.

In practice, the use of law enforcement powers to actively search for financial information and conduct financial investigations outside the framework of cooperation with the FIU and on the basis of intelligence information that the FIU has already received, is yet to be fully validated. In other words, the usefulness of information obtained though trans-national cooperation for initiating and conducting formal investigations into ML/TF cases is yet to be clearly demonstrated.

In previous years, Montenegrin FIU has been bank-focused mostly. FIU has noted cases of local companies receiving significant loans from their parent companies or offshore companies. In most cases, the loans are never repaid to the offshore lender but are used for the purchase or construction of real estate in Montenegro instead. Based on the existing cases, including high-profile E-commerce case, criminal organizations and individuals also often use phantom companies to present fictitious transfers of goods and services in order to legalize or re-direct invested money prefer using electronic transfers based on fictitious accounts mostly opened by foreign nationals instead of using bank notes.

They also used to deposit the proceeds of illicit transactions into offshore accounts and taken back the funds in the form of loans, which they never repay. According to Montenegrin FIU, most illegal proceeds come from Russia, Italy, Switzerland, Serbia, Croatia, and Panama. In a form of service-based laundering, offshore companies send fictitious bills to a Montenegrin company (for market research, consulting, software, leasing, etc.) for the purpose of extracting money from the company's account in Montenegro so funds can be sent abroad.

In many cases, suspicious financial transactions are operated through foreign off-shore financial institutions, located in the British Virgin Islands, Cyprus, the Seychelles, Panama, and Switzerland, which are not easy to follow, because of the lack of capacities and means to investigate the bank accounts abroad. Information technology, electronic transfers, credit cards, internet payments, cyber-currencies, and other new payment methods make these threats more difficult to detect. The potential for enhancing anti-money laundry efforts of the Government lays in further strengthening of crime intelligence anti-money laundering work, including through application of high technology for encrypting communication and monitoring systems of electronic payment over the internet.[175]

- **FIU-to -FIU cooperation**

The FIU conducts exchanges od information and data based on the principles of the Egmont Group, and for it uses the appropriate channels, including cooperation with liaison officers from other countries, and the use of indirect channels available for exchange with Interpol and Europol and international agreements. In order to strengthen international cooperation, according to available data, Montenegro has so far signed 35 co-operation agreements with EGMONT group member states.[176]

In line with the Egmont Group standards on exchange of information among FIUs, Article 68 of LPMLTF stipulates that for the purpose of international cooperation FIU can conclude agreements with authorized bodies of foreign states and international organizations on the exchange of financial

[175] https://www.state.gov/2021-incsr-volume-ii-money-laundering-as-submitted-to-congress/

[176] For example, Montenegrin FIU has signed an operational cooperation agreement with the FOS of Azerbaijan, while being removed from EGMONT group, to facilitate FIU-to-FIU cooperation.

intelligence, information and documentation, which may be used only for the purposes specified in this law. Article 70 of the LPMLTF provides for the conditions under which the FIU of Montenegro responds to foreign FIU requests, including an exhaustive list of the grounds for refusal.

The financial intelligence unit may request from the authorities of another foreign state that are responsible for disclosure and preventing money laundering and terrorist financing to provide data, information and documentation relevant to detection and prevention of money laundering and terrorist financing. Data, information and documentation obtained in this way can be used exclusively for the purposes determined by this law and not without prior consent of the authorities of a foreign state from which they were obtained.

The FIU has the authority to request information from obliged entities at the basis of the request received from a foreign FIU, which contains sufficient grounds for suspecting that money laundering and related predicate offenses or terrorist financing are in question. Subject to reciprocity, it also has the authority to temporarily suspend or postpone the execution of the suspicious transaction as per the request of the other FIU. As per the new LPMLTF from 2019, **FIU can provide information also on the underlying predicate offences**. Before submitting any personal data, FIU shall contact the agency responsible for the protection of personal data to check whether personal data protection standards are protected and the data used only for the requested purpose.

All requests submitted to FIU are sorted by priority, depending on the criminal offence in question and the type of request made, as well as in accordance with the principles applicable to the exchange of information, using the GoAML system - international exchange information and the FIU function related to intelligence and analytics.

As per the Annual Report of Montenegrin FIU for 2020, a total of 93 requests from foreign FIUs were received last year, including 9 from Cyprus, 7 from Russia, 5 from UK, 4 from Germany, 4 from Spain and from Ukraine, 3 from Austria, 3 from Bulgaria, 5 from Slovenia. When it comes to neighboring countries, 17 requests came from Serbia, 4 from Croatia, 4 from Kosovo, and 1 from Albania. Based on this information, 43 cases were established.

- **Mutual Legal Assistance (MLA)**

Montenegro is a signatory to a number of multilateral conventions in the field of mutual legal assistance in criminal matters. The most important among these are the conventions of the Council of Europe: the European Convention on Mutual Assistance in Criminal Matters and its two Additional Protocols, the European Convention on Extradition and its two Additional Protocols, the European Convention on the Transfer of Sentenced Persons and its Additional Protocol, the European Convention on the Transfer of Proceedings in Criminal Matters.

With a view to ensure better and more accurate regulation and to simplify and accelerate the process of providing MLA in criminal matters, Montenegro signed a number of bilateral agreements with the countries of the region, with which the exercise of legal assistance is the most frequent, such as Serbia, Bosnia and Herzegovina, Croatia, Italy, North Macedonia, and is also intensively working to expand the number of countries with which these issues are governed by bilateral agreements. Thus, in order to conclude bilateral agreements with these countries, negotiations are underway with Albania and Kosovo.

In the event that an issue that arises in the relations between two countries is not regulated by a bilateral agreement or multilateral conventions to which Montenegro and the other country are parties, these issues are resolved in accordance with national laws.[177]

[177] The most important regulations regarding the judicial cooperation in criminal matters are the Law on Mutual Legal Assistance in Criminal Matters, Criminal Procedure Code, Law on Prevention of Money Laundering and Financing of Terrorism, Law on Witness Protection, Law on Liability of Legal Persons for Criminal Offences, Law on Internal Affairs and the Law on Courts.

The Law on Mutual Legal Assistance in Criminal Matters[178] stipulates the conditions and procedures for the provision of mutual legal assistance in criminal matters. The Law establishes rules and procedures for acting upon letters rogatory that Montenegro receives and the letters rogatory for mutual legal assistance submitted by Montenegro to a foreign country, depending on the existence of an international agreement.

The Law is of general nature and deals with extradition, transfer of proceedings (assignment and assumption of criminal prosecution), the recognition and enforcement of criminal judgments and other court decisions, as well as with other forms of mutual assistance. The Law restricts the use of "personal data" to the purposes of proceedings for which the information is sought, through which, among other things, it meets the standards needed for cooperation with EUROJUST (Montenegro signed Bilateral Agreement with EUROJUST in 2016).[179] In 2020, State Prosecutor's Office of Montenegro cooperated with EUROJUST in 58 cases.[180]

Joint investigation teams and delivery of banking data are provided as a special form of mutual legal assistance, which is in accordance with the provisions of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters.

In 2019, a special chapter dedicated to joint investigation teams was introduced, as one of the most effective instruments in the fight against cross-border crime, and in accordance with the Second Additional Protocol to the European Convention on Mutual Assistance. The provisions of this international agreement are specified by stipulating rules in regard structure of JIT, how the investigation shall be conducted in Montenegro, conditions for participation of team members from foreign countries, etc. The agreement should be signed by the Supreme State Prosecutor of Montenegro, of which he informs the Minister in charge of Justice.

Also, the transitional and final provisions of the Law refer to the due application of the Criminal Procedure Code, which indirectly affects the process of providing mutual legal assistance. These umbrella laws for providing mutual legal assistance fully meet the procedural prerequisites for the application of the above conventions ratified by Montenegro. Montenegro also adopted Law on judicial cooperation in criminal matters with the EU Member States, which will enter into force on the date of Montenegro' accession to the European Union.

When it comes to international legal assistance in numbers, 1,020 letters rogatory were recorded, out of which 423 foreign requests were sent to Montenegro and 597 requests were sent by Montenegr5in authorities to foreign competent authorities. Montenegro had a larger number of letters rogatory sent to states EU members than it has received.[181] This ratio is the opposite of a ratio between sent and received letters rogatory exchanged with the countries of the Western Balkans, but also with third countries. Most of the rogatory letters to Western Balkan countries concerns criminal prosecution by the Montenegrin State Prosecution. [182]

- **Asset Recovery International cooperation**

The segment of international judicial cooperation that is carried out asset recovery is normatively introduced by the Law on seizure and confiscation of material benefit derived from criminal activity. The Law gives priority to cooperation that is exercised in accordance with a ratified international

[178] „Official Gazette of Montenegro", No. 4/2008, 36/2013 i 67/2019.
[179] The liaison prosecutor at EUROJUST was appointed in December 2017 and re-appointed in November 2019.
[180] Annual Report of the Prosecutorial Council for 2020, https://www.pravosudje.me/vrdt/sadrzaj/a0ww
[181] Annual Report of the Ministry of Justice for 2019, page 5, https://mpa.gov.me/biblioteka/izvjestaji, Report for 2020 not available.
[182] In 2014, the Ministry of Justice of Montenegro, with support of the Dutch Embassy, launched a project to introduce a system of registration of MLA cases - LURIS, which enables precise tracking of the number of received and sent request. LURIS was built in January 2015 and operates effectively as of 2016. Reporting is possible by the type of legal assistance, the criminal offense, the requesting State, the competent authority for taking action and other parameters needed to closely follow the provision of legal assistance. LURIS also allows for merging of the data in one database, and for share of to state prosecutor's documents in electronic form, in line with EUROJUST personal data protection standards.

agreement in relation to the provisions of this law relating to the provision of international legal assistance.

In addition, the principle of reciprocity in the provision of international legal assistance has been introduced, in the absence of an international agreement. The law determines what is included in international cooperation in the subject area (identification, tracking and tracing material benefit, imposing provisional measures to secure assets, seizing movable property, confiscating material benefit, and managing the seized and confiscated material benefit), as well as preconditions for providing international legal assistance, the manner of submitting the request of the foreign body for cooperation.

It is envisaged that the request of the competent foreign authority for mutual cooperation shall be delivered to the competent body of Montenegro through the public administrative authority competent for judicial affairs, and vice versa. The police unit competent for financial investigations shall act upon requests in accordance with the Council Decision 2007/845/JHA of 6 December 2007.

The provisional measures to secure assets shall last until the end of the criminal proceedings, ie the procedure for permanent confiscation of property in the requesting state. The law limits the provisional measures upon the request of a foreign state to a period of two years as of the date of issuance of the ruling imposing a provisional measure to secure assets, provided that this period may, for justified reasons, be extended for another year.

Regarding information exchange for the purpose of financial investigations, Montenegro' participation in the CARIN (Camden Asset Recovery Inter-agency Network) network is important, as well as ARO network through contact points designated in the Police Directorate and in the Prosecutor's Office. As regards property confiscation, especially during financial investigations, the rapid flow of operational information is crucial as a basis for judicial cooperation, aimed at freezing potential crime proceeds.

- **International police cooperation**

**M**ontenegro has established a strong cooperation with Interpol and Europol. The Schengen Information System is incorporated into the national database and the Secure Information Exchange Network Application (SIENA) is used as a national case management application for automatic communication with Europol.[183]

Police Unit INTERPOL – EUROPOL – SIRENE is also being used to facilitate cross-border cooperation in ML/FT cases, as it is responsible for broad operational exchange of information, through police cooperation agreements and participation in joint investigation teams. In 2020, FIU sent 249 requests through this Unit, 131 through Siena and 118 though Interpol/communication with NCB/ liaison officers. On these occasions, checks of natural and legal persons were requested through police and other records, including data on ownership structures of legal entities and all other useful data. The Police Unit INTERPOL – EUROPOL – SIRENE submitted to FIU a total of 132 acts received through international police cooperation.

[183] Montenegro 2019 Report, page 35

# CONCLUSIONS AND RECOMMENDATIONS

Montenegrin authorities have established a comprehensive system and are making significant efforts to provide a wide range of various forms of international cooperation, including through mutual legal assistance, international police cooperation and FIU – to – FIU cooperation. **However, it is still not fully clear how data and information obtained through international cooperation channels are used effectively in the criminal prosecution of these criminal offences in Montenegro.**

It seems that the cooperation is most developed at the FIU-to-FIU level, as well as at the level of operational police cooperation, and also because the secrecy of investigations does not allow for the presentation of such data at MLA level. **However, the number of cases and judgments in the field of money laundering and especially terrorism financing, is so small that it cannot have a deterrent character and effect, not prove the effectiveness of the cross-border cooperation to a larger extent, although that does not necessarily exclude the existence of comprehensive data exchange at the operational level.**

Requests for MLA in Montenegro are processed through a centralized body in charge of MLA in the Ministry of Justice, with participation of Prosecutor's Office and the courts and with certain possibilities for use diplomatic channels also available. MLA is provided in a timely, constructive and effective manner. However, in certain cases, occasional delays have been noted in reaching the competent enforcement body in the foreign country, due to **missing bilateral agreements on the provision of international legal assistance**, with countries with which it has not yet been signed. The work on signing other necessary bilateral agreements should be intensified, including with Albania and Kosovo, to prevent possible delay in MLA proceedings.

Bearing in mind the fact that the introduction of new legal institutes in the field judicial cooperation to increase the scope of legal assistance upon accession Montenegro to the EU, it is necessary to plan an increase in the number of officials who are deal with these cases;

It is necessary to encourage judicial bodies to use direct communication between judicial authorities in MLA proceedings, if provided for by cooperation Agreements or based on the principle of reciprocity.

The new ICT system in courts which is currently being developed in line with ICT Strategy in Judiciary should be made compatible with LURIS.

Information exchange between Montenegrin FIU and foreign FIUs and law enforcements authorities is conducted effectively, on the basis of the Charter of Egmont Group and/or bilateral agreements or memoranda of understanding. It concerns ML/TF as well as related predicate offences. **Cross-border feedback to obliged entities on reports that have been forwarded by an FIU to another FIU, however, appears to be nonexistent or not adequately reported.**

Adequate **level of data protection** is met by the adherence to the relevant points of the Principles of Egmont Group, EU data protection standards and relevant national legislation.

International police cooperation with INTERPOL and EUROPOL and based on bilateral agreements are also being used effectively, to supplement the cooperation of FIUs with foreign counterparts. **This modality of cooperation and information exchange has been especially useful during the period when Montenegrin FIU was not been a member of EGMONT, until participation in this Group was re-established in 2020**, as it was, in addition to MLA, the only channel of cross-border data exchange for FIU.

Capacity of the country to respond to evolving AML/CTF regulatory requirements has evolved significantly in recent years. **As regards FATF Recommendation 40 (Other Forms of Cooperation)**

**and SR.V (International Cooperation), Montenegro addressed most deficiencies noted in 2015, and is considered to have achieved the „largely compliant"(LC) level of compliance with R.40, with some adjustments to be made before the 5th mutual evaluation round.** General shortcomings in terms of access to information, however, still affect FIU's ability to establish a comprehensive and timely cooperation in some circumstances, especially when it needs to use information from external sources. This also concerns the register of real property and lack of interconnectivity among data basis that still impact on the quality and scope of cross- border cooperation.

**Montenegrin institutions should ensure better use of specific statistics available in the field of AML/CTF and should clearly report how information obtained through cross-border cooperation channels has been used for criminal prosecution of ML/TF.**

Setting criteria to determine the types of cross-border cases suitable for joint analysis among FIUs at the cross-border level can also be beneficial to identify a common ground for the "analysis" function to be performed and to allow for better coordination among the work of different FIUs**.**

The implementation of international restrictive measures, established by UNSCR 1373 (2001) and UNSCR 1267 (1999) remain ineffective, especially when it comes to the establishment of overall compliance monitoring system and to imposition of targeted financial sanctions based upon suspicious transactions reports (STRs).

**Montenegrin authorities should ensure that cases containing elements of MLA enjoy systemic priority with all competent institutions on the basis of strengthened internal procedures and management systems, focusing more on terrorist financing, and developing and implementing a comprehensive strategic risk mitigation mechanism for FT.** Technical expertise and experience of other countries in implementing FT Convention as well as other relevant information may be obtained from more developed countries.

german cooperation
DEUTSCHE ZUSAMMENARBEIT

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

# Assessment

## of data protection framework in anti-money laundering regulations

*(Interviews report)*

TRANSPARENCY INTERNATIONAL MACEDONIA

# SUMMARY

Country experts conducted 10 interviews between 9 and 19 march 2021 aimed on providing assessment of the legislative and institutional approximation with the 4th and 5th EU Anti-Money Laundering Directives with a focus on data protection. Interviews were conducted by Montenegrin country experts, Biljana Papović and Ivan Vukcević.

Interlocutors were representatives of relevant institutions, international organizations and civil society that are included in anti-money laundering activities as well as strengthening legislative framework in this area; Directorate for Prevention of Money Laundering and Consumer Protection in the Central Bank of Montenegro, Tax Administration, Data Protection Unit / Ministry of Interior, Police Directorate, Sector for Prevention of Money Laundering and Terrorist Financing, Council of Agency for Data Protection, Agency for Prevention of Corruption, Council of Europe Office in Montenegro, Network for Affirmation of NGO Sector, Center for Democratic Transition.

Questionary was prepared by country experts and included group of questions related to assessment of AML/DP legislation in relation to the harmonization of the national legislative framework with provisions of 4$^{th}$ and 5$^{th}$ directives of the European Parliament and the Council, legal shortcomings, level of regulation of personal data protection during a money laundering investigations, institutional framework and cooperation, international cooperation, quality of risk assessment, law implementation oversight, but also question related to functioning of registries defined by law (Registry of beneficiary owners, politically exposed persons).

Assessments sre based on data and statements of the interlocutors, comparison of the actual situation with the legal framework and analysis of compliance with the relevant directives of the European Parliament and the Council.

The conclusion drawn from the conducted interviews indicates a high degree of commitment of Montenegrin institutions to the process of harmonization of legislation with directives, while in the area of implementation there is still a lot of room for improvement.

The Law on Prevention of Money Laundering and Terrorism Financing (LPMLTF) is almost completely harmonized with the Directive 2015/849, the part that is not harmonized concerns the misdemeanor responsibility and the amount of fines, which are more closely prescribed by the law on misdemeanor proceedings. Harmonization with amendments to Directive 2015/849 brought by Directive 2018/843 are not full achieved, especially when it comes to access to beneficiary owners register.

Montenegro started incorporating the newly introduced standards only a year and a half after the Directive 2019/1153 entered into force, by establishing a working group to draft a new Law. In this moment Law is not harmonized in provisions that regulates establishment of central register of bank accounts, cooperation with Europol, etc.

In the field of data protection, The Data Protection Law (LPDP) is fully approximated with Directive 95/46/EC, it is mainly approximated with Regulation 2016/679 of the European Parliament and the Council, as well as Directive 2016/680. According to our interlocutors, the protection of personal data still depends on the will of the managers of the institution and their awareness of the importance of protection. In preparing a new law that should bring greater harmonization with aquis communitaire, the institutions express concern about the readiness of the system to implement this modern law.

The assessment of the situation in which our interlocutors made a special contribution is the starting point for the preparation of conclusions which are an integral part of this report.

## Legal framework assessment and harmonization with provisions of directives of the European Parliament and the Council

Our interlocutors find that the drafting of the LPMLTF has been done with a view to ensuring harmonization with EU directives. The Law is almost completely harmonized with the 4th Directive, and we started incorporating the newly introduced standards only a year and a half after the 5th Directive entered into force. Amendments to the new LPMLTF are currently being drafted. The new Law will even incorporate penal provisions and sanctions for ML/TF envisaged by the 6th directive that is yet to enter into force. The continuous commitment and obligation to harmonize the legislation in this area with international standards has been observed. It is also noteworthy that decision-makers have been strongly supporting these amendments.

The interviewees are with the opinion that it is very important to adopt a bylaw on electronic identification of persons, which will regulate the opening of accounts remotely and provide for submission of all data in electronic form. It is also necessary to improve the legal framework on games of chance, given the absence of political will to regulate this area in the previous period.

The COE has been providing support to the FIU and the working group for the harmonization of LPMLTF with the 4th Directive, which has been accomplished with the current law. Harmonization with the 5th Directive is now underway, still closely monitored by COE experts. Initial recommendations have been embedded in the new law and institutions remain open to further COE proposals in this area, but the challenge is in making them compatible with other pieces of legislation.

It is commendable that Montenegro is working on integrating the 5th AML Directive into the law. In addition, not all EU countries have fulfilled recommendations from the 4th Directive, which is now the subject of COE analysis. Despite compliance of Law itself, the implementation of LPMLTF in Montenegro in many provisions is still pending.

At the same time, personal data protection standards had to be taken into account throughout the entire drafting process. The recommendation made by COE expert that personal data of clients be retained by subjects of application of Law for no longer than 5 years, in accordance with international standards, was not adopted. The data retention period is currently set at 10 years, after which the data is expunged. The efficiency of the system and its implementation will be best assessed in the course of the 5th evaluation round by Moneywall due in 2023.

Representatives of the civil sector positively assess the readiness of institutions to improve the legislative framework, especially the FIU and the CBCG, which initiate and promote changes. They are proactive, cooperative and professional. The problem in fact lies with the senior level, as ministries only recognize the importance of LPMLTF when they receive a warning from international community. The “red lamp” for harmonization is only activated after increased surveillance measures are imposed or after receiving a threat of a grey list. Objections are particularly aimed at the work of the Ministry of Finance and the Ministry of Foreign Affairs. The Ministry of Finance proposes the Law on Games of Chance, which must undergo a serious reform, given that it regulates an area of particularly high risk.

Apart from LPMLTF, the drafting of a new LPDP is also underway, and it will incorporate provisions of the Regulation 2016/679 of the European Parliament and the Council, as well as Directive 2016/680.[184] The Government envisages the adoption of the Proposal of the LPDP in the fourth quarter of 2021, to be harmonized with General Data Protection Regulation.

Institutions, subjects of application of LPDP and the civil sector expressed great interest in working

[184] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

together to draft the Law. As many as 40 entities participated in the public discussion, after which a 280 pages long report was produced.

Our interlocutors believe that competent authorities are declaratively committed to the harmonization of national laws with EU personal data protection provisions. In most countries, personal data protection falls within the remit of a department within the Ministry of Justice. In our country, it is the Ministry of Internal Affairs that is in charge of this subject matter.

## Shortcomings in the AML/DP legal framework

First our interlocutors point on the main definitions of the most important terms in the AML/DP laws, assessing whether they are clear and comprehensive enough (beneficial owner, politically exposed person, financial institutions, personal data, compliance, processing - processor-user of personal data.

The definitions from Directive 2015/849 have been incorporated into the current Law on the Prevention of Money Laundering and Terrorism Financing. Definitions from Directives 2018/843 and 2019/1153 are included in the draft proposal of the law drawn up by the FIU.

The interlocutors pointed out that the definition of a politically exposed person in the law is broad and going beyond international standards. The term is not synonymous with public official, which is often overlooked in Montenegro. Unlike public officials, politically exposed persons do not have to be Montenegrin nationals, they can be employees of embassies, international organizations, etc.

There are many issues with the current LPDP, that should be amended in order to bring the necessary improvements and harmonization with EU legislation and Directives.

Consent for use of personal data is rather used in private-sector activities, not in the public sector. In the protection of personal data, special attention should be paid to the purpose of limitation. In our country, banks ask for personal data (identification number) due to suspected money laundering even in cases of one-off payments of several hundred euros, which is problematic.

Interlocutors from the institutions did not point out the shortcomings of the legal framework on the prevention of money laundering, on the contrary, they find that it is already largely in line with the Directives, or else that harmonization is underway. Directive 2019/1153 is not incorporated in the current Law on Prevention of Money Laundering and Terrorism Financing. According to their statement new LPMLTF is being drafted, Directive 2019/1153 and Directive 2018/843 are fully ”embedded” in the draft law prepared by the Financial Intelligence Unit (FIU).

The obligation to register beneficial owners is indeed set out in the current LPMLTF, but no deadlines are specified for such registration by companies that are already entered in the Central registry of business entities (CRPS). The current provisions can be interpreted as requiring registration for new applicants only. There is no obligation to re-register, nor a deadline by which to match the data. These issues cannot be prescribed by a rulebook because a rulebook cannot be more prescriptive than the law in force.

There is a major problem with supervision into the work of public notaries and lawyers. Chambers do not have the capacity to conduct supervision, according to our interlocutors assessment. They do not conduct inspections or report problems. This is especially true for Bar Association, which even refuses to supervise and report suspicious transactions, citing attorney-client privilege, although there are absolutely no grounds for this. The Notary Chamber controls the work of public notaries, and thus slightly outperforms Bar Association in this respect, but neither one performs AML controls. The suggested solution is to transfer supervision onto the judicial inspection. However, lawyers do

not want government oversight. In the performance of supervision, the COE gives preference to the Ministry of Justice rather than the Police Directorate.

Issues have also been found with the Law on Games of Chance, as it should first of all provide that persons facing criminal proceedings may not be casino owners. The setting up of a register of beneficial owners will be of great value in this area as well. Supervision over the operation of games of chance is just as problematic, because they cannot be controlled by the Directorate for Inspection Affairs, as they are not sufficiently familiar with risk factors, nor do they have the staff and expertise to supervise risk in these operations.

Virtual currencies, cryptocurrencies and electronic identification will also be regulated by the new Law. Given the scope of the necessary changes, it seems that an entirely new law is a better option than amendments to the existing one.

Representatives of the business sector believe it necessary to remove business barriers, as administrative burden discourage prospective investors in Montenegro. However, the introduction of incentives would be contrary to the Directives. Further improvement of the e-signature and eID system will be beneficial in this area.

## Personal data protection in scope of money laundering investigations

The feedback regarding system of data protection in money laundering investigations was a positive one, with expectation of further improvement. Not every institution is facing the same implementation challenges.

The CBCG is not faced with too many challenges, controls and supervisions of reporting entities. Special attention is paid to data safeguarding. The activities of employees in this respect are regulated by internal acts.

Personal Data Protection Agency (AZLP) made a recommendation regarding data exchange and data protection to Tax Administration (regarding CRPS, but this will also apply to the register of beneficial owners) - to protect the ID number and address of a natural person involved in a company. This recommendation has been implemented in the system, and Tax Administration ensures that data contained in excerpts issued to third parties are protected. The Tax Administration does not have internal procedures for data protection. All employees can access vital records internally, which is an area of risk and requires special attention. Independent clerks are operators who enter data from applications for registration in the CRPS. However, they do not have access to the database, as there are several levels of access. On the other hand, all employees must have access to personal data as they are relevant for different parts of the system. As for the register of beneficial owners, after an applicant submits data, they are to receive a signed form and an excerpt that is generated by the system. There is no contact with officers, so the risk of misuse of personal data is reduced. Also, not all employees are granted access to this register, only a designated sector in charge of its maintenance. So far, no reports of misuse of personal data by Tax Administration have been submitted by parties, i.e. companies entered in the register.

There is a special internal connection for communication between the FIU and obligors. Data delivery is done via a secure network. There is a high level of security and protection. As a member of Egmont, the FIU must abide by the principles and rules prescribed within the network. There is a department that has access to the exchange channel and which receives and forwards data obtained from administration authorities. The principles are extremely strict, and field evaluators check for compliance. The scope of compliance checks ranges from independence - whether the systems are effective for personal data protection, protection of classified data, whether there are

security zones, whether the person accessing them is identified, implementation of rules on data safeguarding and storage in the manner prescribed by international standards. Upon restoring its membership in Egmont, Montenegro passed the evaluation and was assessed as having met all the necessary conditions.

## Institutional framework and capacities

The general assessment of interlocutors on the current institutional framework was a positive one, with a note that the identified shortcomings are already being actively remedied in the new proposals of the law that are currently being drafted. Representatives of the civil sector positively assessed the fact that the work on improving legal framework in the area of AML and DP is being done in parallel.

Interviewees expect that provisions of the new law, which stipulate that each organization is to designate a data protection officer, are to bring improvement in raising awareness of the importance of DP, however, question remains as to the extent of practical implementation.

The general assessment is that all of the authorities need to improve knowledge of the subject matter. One of the interlocutors proposed that Prosecutor's Office might also designate a prosecutor with expertise in the field of personal data protection.

Our interlocutors were critical towards the notion of a collegial body (the Council of the Agency for Personal Data Protection), deeming it an unfit solution and claiming that it should be one person at the top instead.

Preparation of new LPDP raised concern of institutions regarding challenges in the future implementation of the new solutions. This go along the lines of whether authorities and reporting entities will be prepared for these technical solutions, how the deployment of these modern IT solutions is going to work, and what budget allocations will be set aside for this purpose.

Currently, the level of personal data protection in Montenegro depends on the managing staff of an institution and their willingness to apply the law. The key person for ensuring that the law is implemented is the manager, which basically means that the awareness of personal data protection within an institution depends on the will of whoever is in charge.

## Institutional cooperation

An inter-institutional cooperation agreement (internal act) for automatic exchange of data was signed between the Ministry of Interior, the Ministry of Justice (including criminal records), the Ministry of Finance (including Tax Administration and Customs Administration), the Supreme Court and the State Prosecutor's Office. The Agreement is being amended so as to include the Central Bank. An efficient web service has been established, which guarantees data protection, with access restrictions, logging records and user identification. The application maintained by the FIU records who accesses it, when, on what legal basis, followed by a description. It also records who accesses the data, based on which act and notes the reason. Data are not being exchanged between the FIU and State Prosecutor's Office. As for other authorities in question, the data exchange is running uninterrupted. Prosecution's IT system has compatibility issues. The FIU is making extensive use of data from other authorities, all the while in line with the applicable LPDP. So far, no reports of abuse of the data exchange system have been recorded.

Cooperation between the FIU and the CBCG has been established in 2014. CBCG and PD signed a bilateral cooperation agreement in 2019. The agreement clearly prescribes obligations and responsibilities. The cooperation was assessed as excellent, from joint work on amendments to the

Law, weekly communication, arranging joint actions, to taking part in joint trainings. Cooperation between the FIU and the CBCG is very important in light of the 5th AML Directive. It includes data that are necessary for the FIU, primarily the register of accounts and safe-deposit box holders. The register will be kept by the CBCG, but the primary Law regulating the register is the Law on Prevention of Money Laundering and Terrorism Financing. The 5th Directive stipulates that there shall be no anonymization of holders of bank accounts and safe-deposit boxes. The register of beneficial owners is also regulated by the LPMLTF, and this register is kept by the tax authority.

There is currently no access to data and data exchange between the FIU and the Real Estate Administration, but this too is underway. For now, the FIU uses the publicly available REA database or else submits a request.

## International cooperation

Communication and data exchange have been greatly accelerated after the establishment of the FIU within the Police Directorate, and after Montenegro rejoined the Egmont system following evaluation. EGMONT is protected and efficient. Bilateral data exchange was difficult and complicated. FIU is also using the SIENA system.

Representatives of the civil sector, on the other hand, believe that membership in EGMONT alone is not crucial for the exchange of relevant data. They point out that a lot depends on the country receiving the request. Some countries are responsive, others are not. The exchange of information depends not only on the legal basis but also on the political will. Equally important is the subjective aspect i.e. the trust in the FIU. If there is a slightest doubt regarding its security or access, countries will not share the data. They may delay or send unusable data if they happen to distrust the FIU. The bottom line is that Egmont members are extremely well acquainted with the situation in the country, as well as with institutional integrity.

AZLP previously cooperated with the EDPB and the Berlin Telecommunications Group, but this is not the case anymore. The Law on Internal Affairs and International Agreements regulates cooperation of the Ministry of the Interior. Cooperation with international organizations was positively assessed during the drafting of the Proposal of the Law. The support is mainly provided by experts from Slovenia and Croatia because they are most familiar with our system.

## Quality of risk assessment

The national risk assessment was done with the support of the COE. The quality of this document varies, depending on a particular area and the competent authority. Financial institutions did a good job, while the non-financial sector was assessed to be underperforming in this area. The conclusion is that the new national risk assessment is better than the previous one, with room for further improvements.

The national assessment should serve as the basis for drafting sectoral risk assessments, which are to be regularly updated in order to make way for surveillance plans. This is not being done in our country, there are no sectoral plans nor sectoral assessments (for financial institutions, non-financial institutions, public notaries, lawyers, games of chance, etc.). Interviewees have pointed out that Montenegro is not an isolated case in this respect, but that this is a widespread problem given that these assessments are not being done at the EU level either.

The problem is that national risk assessments are done for a period of 5 years, during which time significant changes may occur. A key obstacle to producing a shorter-term national assessment is the inadequate updating of statistical data.

Our interlocutors find that it is necessary to improve the cooperation between the FIU and the department of the Ministry of the Interior that performs supervision (Department for Supervision of Prevention of Money Laundering and Terrorism Financing). They need to provide each other with data and monitor changes in risk in order to strengthen supervision, but they are currently operating separately. This arrangement was working better while both departments were under the same authority, but this department could not remain within the Police Directorate because it has inspection powers and not powers of a police body. Basically, the problem of police having no competencies to carry out inspections has been solved by having them performed by the Ministry of the Interior.

CBCG has its own risk management mechanisms. Subject of application of the LPMLTF are also tasked with risk management. ML/TF risk is a reputational risk for banks. It is necessary for management staff of banks and other financial institutions to have greater awareness of the importance of risk assessment. The number of measures applied in the area of risk management has also been increased. There are warning measures, a detailed report on irregularities, which contains recommendations (listing every irregularity the bank needs to remedy). For example, they issue instructions that internal acts need to be adopted or revised, also, reporting entities need to provide evidence that the recommendations contained in the warning have been met. This is an effective way to stir the reporting entities to action, to force them to have a good risk management system in place. CBCG guidelines are clear, they prescribe what needs to be done and how to do it. If fully applied, this system functions well.

## AML/DP legislation implementation oversight

The Central Bank is the supervisory authority for some of the most important institutions in this area (banks, financial institutions, legal entities dealing with currency management). Each reporting entity is assigned an authorized supervisor, and this cooperation functions well. New control rules have met with resistance from bank management due to rising costs. Authorized supervisors are thus caught in the middle between an employer seeking profit and the Central Bank seeking compliance. After the transitional period that is now in effect, stricter sanctions will be issued. We will soon have a risk-based approach in the controls, i.e. we will first perform controls into high-risk banks.

The FIU suggested that the new LMLPFT will introduce changes into oversight over the work of public notaries and lawyers. It is currently functioning on the principle of “the one accusing you is also the one judging you.” Starting this year, the cooperation with notaries has been improved, as notaries are now able to submit data through the designated FIU portal. However, they too believe that the supervision of the work of notaries should be performed by a state institution. The Ministry of Justice is the most logical solution, but it might be another authority, as long as it is working independently from the chamber. The current system which envisaged for the notary chamber to do supervisions is not a functional one because, just as with lawyers, supervisions are not performed and there is no feedback from the supervisory body. Notaries submit data, especially now through the newly-established portal, but there is no insight into whether they submit all of the data, given that there is no supervision.

Supervision over the implementation of the LPDP is performed by the AZLP. Supervision is well regulated in the law, but the implementation falls short. The Agency can perform control into all authorities and has a great responsibility. The only exception is the intelligence service (only a control into their procedures can be performed). There are four types of control - parliamentary, governmental, internal and independent control (Ombudsman and Personal Data Protection Agency). The understaffed AZLP is cited as an obstacle to establishing a more efficient system.

The sector for games of chance remains to be better regulated by the new law. The FIU has proposed that the sector should be supervised by the Administration for Games of Chance. Supervision is currently carried out by the Directorate for Inspection Affairs (it has been seen in practice that they lack specialized expertise). In line with the new law, the Directorate for Games of Chance will be issuing licenses, so it would only make sense for the issuing authority to also perform the supervision, as is the practice in EU countries.

## Establishment of a register of beneficial owners

The register of beneficial owners has not yet been established in Montenegro. The legal deadline for establishing the register is one year, and the competent authority is the Tax Administration. The Tax Administration expects to establish the register within this legal deadline. The register will feature the possibility for submitting applications electronically. A user guide has been prepared for both electronic and physical registration, and a promotional campaign is in store.

The Rulebook, which regulates the Register in more detail, was prepared after the 2018 amendments to the LPMLTF, but the recommendation was to wait for the adoption of the new Law in December 2020. The Rulebook elaborates technical details on registration and access levels of certain user groups. Our interlocutors cite the neighboring Serbia as a positive example, given that they adopted a separate law on beneficial owners.

All the steps have been taken, an external software development company has been hired, the application is expected to be completed by the end of March and data entry could start immediately.

In this respect, the Tax Administration is the authority in charge of registration, i.e. record-keeping but is not responsible for the accuracy of the entered data, nor does it control data validity. The applicant is responsible for the validity of the data. The burden of proof does not lie with the tax authority.

There are several levels of access to the register according to LPMLTF. The FIU has full access, while persons who provide justification for legitimate interest can be granted access upon payment of a fee. Law prescribes that the request for access proving a legitimate interest should be sent to the Tax Administration, which then forwards it to the FIU. Subsequently, the Tax Administration will act upon a decision issued by the FIU, to an extent specified in the decision.

CRPS is linked to the register of beneficial owners. It will be linked to the central population register, and it is also planned to establish a link to the tax register. The entry into the register is performed by entering ID number / TIN, and the data is imported automatically, and a check is performed into whether the data match. If there is no match, it is necessary to first submit a request to change the data in the vital records and only then can the application be submitted into the register of beneficial owners.

Interlocutors from the civil sector point out that it cannot be concluded from the available data whether the Tax Administration has fulfilled its obligations and established the Register of beneficial owners, let alone whether the Register is functioning, who are the data users and who is performing control.

Unfortunately, the Law stipulates that the Register of beneficial owners is not available to the public. It is envisaged that the data from the register are to be made available only to the authorities, while other legal entities and individuals will have to prove a legitimate interest in order to obtain information.

This is contrary to the 5th AML Directive, which specifically lists the media and civil society organizations as important users of beneficial ownership information. The Directive states that

public access to beneficial ownership information allows greater scrutiny of information by civil society and the media and contributes to preserving trust in the integrity of business transactions and of the financial system. It also facilitates the timely and efficient availability of information for financial institutions as well as authorities, including authorities of third countries, involved in combating money laundering and terrorist financing. The access to that information would also help investigations on money laundering, associated predicate offences and terrorist financing.

Interlocutors from the competent authorities do not see any obstacles to making the register public even before the amendments to the law in terms of basic data on beneficial owners, in accordance with the 5th Directive.

## Establisment of the register of politically exposed persons

According to LPMLTF, the Agency for the Prevention of Corruption (ASK) maintains the list of politically exposed persons, which is published on their website. After the Law was amended, this list was not compiled and published. Following an interview held with the head of ASK, this institution began work on setting up this register, to be carried out within the 30-day deadline. Data is being collected from other reporting entities in order to complete and publish the list.

Currently, the ASK publishes a list of public officials, but not all of them are politically exposed persons, and also, certain persons who are not public officials are missing from the list.

Each bank is obliged to collect data on clients and check into whether they are politically exposed persons. Based on the collected data, banks develop a risk profile which serves as a basis for transactions motoring. The data of politically exposed persons are to be submitted to the competent authority in charge of their publication. The functionality of this register will be assessed by the completion of the final report.

## Conclusions on the alignment with provisions of directives of the European Parliament and the Council

- The AML/DP legislative framework is being amended to increase compliance with Directive 2019/1153, Regulation and Directive 2016/680
- LMPLFT is aligned with Directive 2015/849, full compliance will be achieved by enacting the penal provisions prescribed in accordance with the Law on Misdemeanors.
- The establishment of a register of beneficial owners is in its final stages, following the legal provisions in accordance to Directive 2015/849.
- Level of access and free access to data should be amended in LPMLFT and accompanying Rules and Procedures, in concordance with amendments from Directive 2018/843. The Directive stipulates that the general public is allowed access to at least information on the name, month and year of birth, the country of residence and nationality of the beneficial owner, and the nature and extent of the ownership interest it holds. The law, on the other hand, requires proof of legal interest. Access by directive should be free, while the Law prescribes the collection of fees.
- Changes to the LPMLTF are necessary, since issues of mandatory re-registration of beneficial owners for existing taxpayers are not regulated by current Law, which must be specified as well as deadlines.

- Establishment of the PEL register, according to recommendations provided by country experts on interview with the Director of Anticorruption Agency has started, in accordance to Directive 2015/849.
- Legal provisions relating to the definition of virtual currencies, cryptocurrencies need to be revised in accordance with the Directive 2018/843.
- Issues related to the establishment of a central register of bank accounts are not regulated by law, which is the subject of regulation of the directive 2019/1153.
- The exchange of information between foi as well as issues of cooperation with europol are not in line with the directive 2019/1153.
- LPDP was amended in accordance with the 2015 Regulation, but not with the Directive.

## General conclusions:

- Awareness of institutions about the need to amend the AML/DP in accordance with EU standards exists, and they are actively engaged in this field
- Awareness of the importance of personal data protection is not at a satisfactory level, it still depends on personnel solutions in the management of institutions
- The implementation of LPDP falls short. Strengthening the institutional capacity in the AML/DP system is a prerequisite for improving implementation.
- System of personal data management within Tax Administration needs assessment and revision, bearing in mind the wide level of access to data for employees, as well as the absence of internal procedures for personal data protection.
- Insight into personal data is to be gained on a basis of LPDP and upon a consent, and not as based on a regulation, in order not to depend on case by case approach.
- The bar in terms of personal data protection, complex data processing and technology should be raised, which should be subject of ongoing changes in LPDP legislation.

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

TRANSPARENCY INTERNATIONAL
MACEDONIA

# Assessment

## of data protection framework in anti-money laundering framework

*(Focus group report)*

# GLOSSARY

| | |
|---|---|
| APC | Agency for the Prevention of Corruption |
| APDP | Agency for Personal Data Protection and Free Access to Information |
| FIU | Financial Investigation Unit (Police Directorate) |
| SSPO | Special State Prosecutor Office |
| MoI | Ministry of Interior |
| CBM | Central Bank of Montenegro |
| TD | Tax Directorate |
| AMLL | The Law on Prevention of Money Laundering and Terrorism Financing (Anti Money Laundering Law) |
| LPDP | Law on Personal Data Protection |
| GDPR | General Data Protection Regulation |
| CoE | Council of Europe |
| EU | European Union |
| LEAs | Law Enforcement Authorities |
| FATF | Financial Action Task Force |

# SUMMARY

Country experts moderated focus group on May 17, 2021 aimed on providing assessment of the institutional and functional approximation with the 4th and 5th EU Anti-Money Laundering Directives with a focus on data protection. Focus group was prepared and organized by Montenegrin country experts, Biljana Papović and Ivan Vukcević.

Interlocutors were representatives of relevant institutions, involved in AML/DP activities as well as strengthening legislative framework in this area: Special State Prosecutor Office, Police Directorate - Sector for Prevention of Money Laundering and Terrorist Financing, Central Bank of Montenegro - Directorate for Prevention of Money Laundering and Consumer Protection, Agency for Data Protection, Agency for Prevention of Corruption, private sector - bank, civil society.

Questionary was prepared by country experts and included group of questions related to assessment of AML/DP practices, in accordance with provisions of 4$^{th}$ and 5$^{th}$ directives of the European Parliament and the Council, interoperability, level of readiness of institutions to meet the requirements of EU directives, the problems they encounter in their work, the functionality of registers of beneficial owners, politically exposed persons, bank accounts. Aim was to evaluate if balance between efficiency in AML investigations and a high level of data protection properly is properly set in practice, and how. International cooperation and procedures was given special attention in this discussion, having in mind the importance of international data exchange in money laundering investigations.

The general conclusion is that institutions are actively working to improve the system when it comes to AML/DP, but these activities, in the context of Directive 5 especially, can only be considered initial. In addition, very rapid changes in this area, at the international level, make it difficult to strike a balance between the legal framework and practice. Some systems work well in practice, although they are not yet shaped by the legal framework, and this primarily refers to the work of FIUs, their communication channels and the way they work. However, some legally recognized institutes have not yet been established in practice (register of beneficial owners and PEL register).

The fact that concrete work is underway to improve the AML/DP legislation, with a precise implementation of the provisions of the Directives, indicates that full compliance, but also the coincidence of practice with the legislative framework can be expected only in the coming period.

Institutional readiness and the will to protect personal data in money laundering investigations exist. Institutions follow what is required by the secrecy of investigations or strict international rules, while consulting the PDP Agency for concerns. In the opinion of the Agency as a supervisory body in this area, human resources in terms of the applicable law exist, although the protection of personal data is still not a key priority in the work of institutions. However, bearing in mind that the current law is still in the phase of change, following the GDPR and EU directives, continuous training at all levels has already crystallized as a need.

Another problem is that full interoperability in data exchange has not yet been established and that much of the work is still done “on paper”, which reduces data security. However, violations and abuses are very difficult to prove in practice, while institutions point out that there was no report or misuse of personal data.

*The Law on Prevention of Money Laundering and Terrorism Financing (LPMLTF) is almost completely harmonized with the Directive 2015/849, the part that is not harmonized concerns the misdemeanor responsibility and the amount of fines, which are more closely prescribed by the law on misdemeanor proceedings. Harmonization with amendments to Directive 2015/849 brought by Directive 2018/843 are not full achieved, especially when it comes to access to beneficiary owner’s register.*

*Montenegro started incorporating the newly introduced standards only a year and a half after the Directive 2019/1153 entered into force, by establishing a working group to draft a new Law. In this moment Law is not harmonized in provisions that regulates establishment of central register of bank accounts, cooperation with Europol, etc.*

*In the field of data protection, The Data Protection Law (LPDP) is fully approximated with Directive 95/46/EC, it is mainly approximated with Regulation 2016/679 of the European Parliament and the Council, as well as Directive 2016/680. According to our interlocutors, the protection of personal data still depends on the will of the managers of the institution and their awareness of the importance of protection. In preparing a new law that should bring greater harmonization with aquis communitaire, the institutions express concern about the readiness of the system to implement this modern law.*

## PROTECTION OF PERSONAL DATA IN MONEY LAUNDERING INVESTIGATIONS THROUGH PRACTICE

The work of the Special State Prosecutor's Office (SPO), which is responsible for prosecuting money laundering offenses, is regulated by procedural laws. Data protection to which prosecutors have access is ensured, reconnaissance and investigations are classified to varying degrees. Until the indictment is filed, all data available to the prosecution from other entities are protected.

When certain data from other state bodies are used, all prosecutors and associates have licenses on the basis of which they access certain databases. Labels range from internally to top secret, and in their work they are guided by it. All in accordance with the Code of Criminal Procedure, other regulations.

Interoperability is not always established. Direct access to databases of Central Bank (CB) and Ministry of Interior is established. Licensed employees of SPO have direct access to databases with login recordings on time, date and scope of information obtained. But problem remains communication with other institutions which is conducted in "paper form". When it comes to AML investigations, not only access to data of other employees is problem, but as well time needed for reply to be secured by relevant institutions.

Also, the problem is the situation that the response to the request of the prosecution is incomplete and that a new round of communication with certain bodies must pass in order to complete the request.

This procedure slows down work of SPO, and for that reason they constantly advocate and insist on connected and accessible databases for all relevant institutions, so that they can obtain the appropriate information at the time of interest. The SPO emphasizes that minutes are crucial in money laundering investigations and that this way of working is not in favor of the efficiency of the investigation.

In the manner of PDP regulations, having direct approach to databases would also secure that personal data be better protected.

On May 7, an Agreement in the field of crime prevention was signed to improve cooperation between the Ministry of Interior, the Police Administration, the FIU, the Ministry of Finance, the Ministry of Justice, the Supreme Court, the Supreme State Prosecutor's Office, the Judicial Council, and the Central Bank. It replaced the agreement from 2017, which was partially respected, ie it was fully respected only by the FIU. Agency for Prevention of Corruption is not part of this Agreement and in following period, according to their proposal, it would be useful to be included. This is very important because RAI recently initiated regional network for exchange of real estate data, which is run by APC.

Automatic data exchange takes place between all institutions. This includes the revenue administration (taxes, customs and games of chance) and data from the real estate administration. The agreement contains precisely stated information that is exchanged and in what way. Also, the agreement contains provisions on mandatory protection of personal data during data processing and exchange.

FIU used to exchange data according to old agreement and still has access to many databases, including databases of police and Ministry of interior, Ministry of Justice, tax administration, Judicial Council, CB. They insist on obtaining access to real estate register, including registration history for a property.

The provisions of Law on PDP itself are largely incorporated into the AML law, implemented by FIU. It prescribes which records are kept, in what way and by which persons the data are used. They have their own completely closed information system which is under full control and positively evaluated by international entities. Data on logging, the amount of information used and the purpose are carefully monitored, both for the internal information system and for access to other databases.

In the opinion of the Agency for PDP, the amount of personal data that is collected is often higher than the needs, which data are needed to achieve the purpose. Personal data protection measures must exist, and every personal data controller must take strict care to ensure these measures and prevent misuse.

All document collection managers and processors must ensure that users of personal data, the data being processed, the legal basis, logins to the system and other data are registered in the information systems.

Institutions in Montenegro often ignore the fact and legal obligation of all bodies to submit to the Agency the registration of records of personal data they have used. The Agency is not interested in a list, scope of data or purpose, but is submitted according to a special form on which legal basis and which personal data the institution collects.

The processing of personal data related to money laundering was not the subject of complaints from citizens for violations of the right to privacy or personal rights before the Montenegrin branches.

In general protection of personal data is not in focus, and one of the priorities of state administration bodies. The Agency for PDP, as a supervisory body, is quite dissatisfied with the attitude towards the protection of personal data by institutions and people who process data.

## LEGISLATIVE APPROXIMATION

It is important that a new law is being drafted that will prescribe additional records kept by the FIU, as well as records related to customs, bank records and safes. The provisions of the AML law concerning the register of beneficial owners will be improved in terms of setting a deadline for the registration of existing legal entities, but also the liberalization of persons who have access to basic data.

When it comes to the new PDP law, it is under the authority of the Ministry of Interior, and the Agency participates in its preparation. It is planned to be done in the IV quarter.

Provisions of the 5 Directive will be part of the new AML law, and according to directive 679/2016, work is underway to harmonize the law on PDP.

Alignment with the GDPR will be part of PDP law, and the Police Directives will be part of the new legal text. This new law also being prepared, in line with Directive 680, which concerns the protection of personal data when it comes to law enforcement authorities. AML law will be harmonized with directives 680 regarding personal data and 1153/2019 on the manner of using financial data.

## The register of beneficiary owners

The register of beneficiary owners run by Tax administration is in the last phase and it will be functional soon. But AML law now has one omission, that it is relevant only for new legal entities, not existing ones. A mitigating circumstance for banks when compiling the register of beneficial owners is the existence of an annual obligation to update data for all non-resident legal entities, and legal entities that have over 25% foreign capital. So they once a year update the data needed to keep tax registers.

## Register of bank accounts

CB responsible for maintaining this register of bank accounts, which is accessible to all relevant institutions. CB takes special care of the protection of personal data. There is an internal rulebook on data protection which is the basis for action. The CB has an obligation to keep the personal data confidential because they represent a banking secret in the relationship between the bank and the client, to which they are obliged by the positive regulations in the field of the bank sector. The logs remain, access decisions by the competent access authorities are necessary and this system works properly.

Currently CB is spreading this database not only to residents, but also non-residents, which could improve AML investigations. This way FIU and SPO could have more efficient approach to database and data obtaining. The central register of safes and the register of remittances will be the subject of a new AML law, under jurisdiction of the CB.

## Register of politically exposed persons

The current AML law, when it comes to the records of politically exposed persons, provides for the creation of a list of these persons by the Agency for the Prevention of Corruption (APC), which will be publicly available on their website. The Agency is in the phase of collecting data in order to publish this list in accordance with the law, and in that process there is no communication with the banking sector, which in the process of opening bank accounts identifies these persons by filling out a personal statement on political exposure.

One sector will be in charge of managing this list, and access will be provided only to persons specially authorized, with the recording of each login as well as the purpose.

From the banking sector it is pointed out that it is important that communication between the Agency for the Prevention of Corruption and banks is established, so that the credibility of statements made by individuals can be verified, and to determine precisely the political exposure of bank account holders.

The FIU point out that the shortcomings of this legal solution (list of PEP) have already been recognized and that changes are underway that the new law will bring changes in this area, and instead of a list, it will enable a functional register, which will be directly accessible to certain institutions and actors.

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Norwegian Ministry of Foreign Affairs

TRANSPARENCY INTERNATIONAL MACEDONIA

# ASSESSMENT OF DATA PROTECTION FRAMEWORKS VS AML/REGIMES IN ALBANIA

**Besa Tauzi**

**Zamira Nurce**

**May 2021**

**Tirana, Republic of Albania**

I. ABBREVIATIONS ..... 160
II. INTRODUCTION ..... 163
III. METHODOLOGY ..... 164
IV. AML LEGISLATION ..... 166
IV.1 Legislation development ..... 167
IV.2 Cross-border cooperation in AML/CTF issues ..... 167
IV.3 Level of approximation with 4th and 5th Directives ..... 169
IV.4 What is still missing to full compliance? ..... 170
V. DATA PROTECTION LEGISLATION ..... 174
V.1 Legislation development ..... 176
V.2 Level of approximation with aquis communautaire ..... 176
VI. AML LEGISLATION VIS-À-VIS DATA PROTECTION LEGISLATION ..... 178
VI.1 Material compliance between AML and data protection legislation ..... 178
VI.2 Institutional approach ..... 182
VII. RECOMMENDATIONS ..... 194

# I. ABBREVIATIONS

| | |
|---|---|
| *AFIU* | Albanian Financial Intelligence Unit. |
| *AML* | Anti-Money Laundering. |
| *ALL* | Albanian Leke |
| *AML Law* | Law no. 9917, dated 19.05.2008 "*On the prevention of money laundering and financing of terrorism*" as amended. |
| *Anti-Terrorism Measures Law* | Law no. 157/2013, dated 10.10.2013 "*On the measures against the financing of terrorism*" as amended. |
| *Convention of the Council of Europe for the Protection of Individuals from automated processing of personal data* | Approved through law no. 9288, dated 07.10.2004 "*On ratification of the Convention on Protection of individuals from automated processing of personal data*" as amended. |
| *Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and Financing of Terrorism* | Approved through law no. 9646, dated 27.11.2006 "*On ratification of the Convention of Council of Europe on laundering, search, seizure and confiscation of proceeds from crime and financing of terrorism*". |
| *Council of Europe Convention on the Prevention of Terrorism* | Law no. 9641, dated 20.11.2006 "*On the ratification of European Council Convention" on the prevention of terrorism*". |
| *Data Protection Law* | Law no. 9987, date 10.03.2008 "*On personal data protection*" as amended. |
| *Directive 95/46/EC* | Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealed by GDPR. |
| *3rd Directive* | Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. |
| *4th Directive* | Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. |
| *5th Directive* | Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. |
| *EU* | European Union. |
| *EUR* | Euro. |
| *FATF* | Financial Action Task Force. |

| | |
|---|---|
| *GDPR* | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). |
| *GTD* | General Tax Directorate, holder of the Registry of Bank Accounts. |
| *IDP Commissioner* | Commissioner for Freedom of Information and Personal Data Protection. |
| *Instruction no. 19* | Instruction no. 19, dated 03.08.2012, of the IDP Commissioner "*On regulation of the relationships between the controller and processor in case of outsourcing of the personal data processing activities and on use of a standard contract in case of such outsourcing*" as mended. |
| *Instruction no. 22* | Instruction no. 22, dated 24.09.2012, of the IDP Commissioner "*On determination of the rules for the preservation of the security of personal data processed by small data processors*" as amended. |
| *Instruction no. 47* | Instruction no. 47, dated 14.09.2018, of the IDP Commissioner "*On determination of the rules for the preservation of security of personal data processed by large data processors*". |
| *Instruction no. 48* | Instruction no. 48, dated 14.09.2018, of the IDP Commissioner "*On certification of the information security management systems, of personal data any their protection*". |
| *Law on Bank Accounts Registry* | Law no. 154/2020, dated 17.12.2020 "*On the Central Registry of Bank Accounts*". |
| *Ministry of Finance* | Ministry of Finance and Economy. |
| *Moneyval* | Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. |
| *NBC* | National Business Center, holder of the UBOs Registry. |
| *Obliged Entities* | Means the obliged entities as per the provisions of the 4th and 5th Directive, the entities as per article 2(14) of the AML Law, the reporting entities as per article 3(5) of the UBO Law and the Financial Institutions as per article 4(5) of Law on Bank Accounts Registry. |
| *Project* | The project carried out by Transparency International Macedonia with the support of GIZ as commissioner by the as commissioned by the Federal Ministry for Economic Cooperation and Development of Germany and the Ministry of Foreign Affairs of Norway "*How the Anti Money Laundering Regulations Respect the Data Protection*". |
| *Registry of Bank Accounts* | Central Registry of Bank Accounts, established in virtue of the Law on Bank Accounts Registry. |
| *Report* | This report. |

| | |
|---|---|
| *GTD* | General Tax Directorate. |
| *UBO* | Ultimate Beneficial Owner. |
| *UBO Law* | Law no 112/2020, dated 29.07.2020 "*On the Registry of Ultimate Beneficiaries*". |
| *UBOs Registry* | Registry of Beneficial Owners, established in virtue of UBO Law. |
| *ToC* | Table of Concordance of Albanian AML legislation with the 4th and 5th Directive, delivered via e-mail as of 25.04.2021, as amended on 20.05.2021. The ToC is attached to this Report as Annex 1 thereof. |

# II. INTRODUCTION

Prevention, detection, investigation and prosecution of money laundering and financing of terrorism have acquired increasing efforts in both, international and national context. Establishment of effective tools and mechanisms to achieve the purpose of preventing, investigating and prosecuting money laundering and financing of terrorism may guide towards paths, which would allegedly deviate from other fundamental rights, if it is not paid the required attention thereto.

Considering the deterrent effect that the traceability of information has on the fight against this phenomenon, the anti-money laundering and countering of financing of terrorism field is being pushed more and more towards transparency and wider access to information. Such access, which must be evaluated from two different perspectives – namely, access granted to the authorities directly involved in the fight against money laundering and financing of terrorism and the access granted to the public – raises issues of a data protection stamp.

In order to not adversely affect the main purpose for which these mechanisms are put in place, which is that of creating a hostile environment to persons that seek rooms to conduct their illicit activities in a non-transparent and bureaucratic system, it is crucial increasing attention on compliance with fundamental rights that would be directly impacted from an increased transparency.

This Report is drafted in the ambit of the Project undertaken by Transparency International Macedonia "*How the Anti Money Laundering Respect the Data Protection*", having into consideration the path of Albania towards accession in the EU. This path implies continuous legislative improvements to reach full approximation with the EU acquis on AML/CFT regime.

The purpose of the Report is to provide countries with timely assessment of the national legal and institutional approximation with the 4$^{th}$ and 5$^{th}$ Directives and the approach that need to be taken vis-à-vis data protection in the AML/CTF regulations.

The Report is limited to the Albanian legislation and jurisdiction and is drafted solely for the purpose of this Project and to the benefit of Transparency International Macedonia as implementing entity.

The Report is drafted based on the understanding of the local experts on the purpose thereof as resulting from the Concept Note drafted and provided to them for this purpose and is the outcome of their understanding and interpretation of domestic legislation in both, AML and data protection domain.

The Report is drafted with a view to present the regulatory and practical issues that arise in connection with AML regime vis-à-vis data protection, from the research and consulting activity conducted by the experts with laws, sublegal acts and case law in Albania, as well as from interviews and Focus Group Discussion held with AML stakeholders in Albania.

Moreover, the purpose of the Report is to be submitted to the AML stakeholders as an input, rather than as country case study, and all reasonable efforts have been put into reflecting, to the most extent possible, a clear view on how the AML legal regime is organized and how it works in Albania towards both 4$^{th}$ and 5$^{th}$ Directive, and towards the Data Protection Law requirements as well.

The Report does not aim at addressing the responsibilities, but rather at providing hints for improving the cooperation and enhance synergies between involved institutions with a view to increase the effectiveness of prevention and combating the illicit activities, and at the same time at ensuring that minimum standards of data protection, as addressed in the 4$^{th}$ and 5$^{th}$ Directives, are ensured in the AMLT regime in Albania.

# III. METHODOLOGY

The Report is drafted based on a combined assessment approach, which includes the material approach reflected in the AML legislation in Albania and the institutional approach of AML stakeholders towards Data Protection Law requirements, the sublegal acts issued on its applicability, and the IDP Commissioner findings in the ambit of its investigations carried out at the relevant public authorities pertaining to the AML domain.

For the assessment of the material approach, the primary and secondary legislation in both AML and data protection domain were consulted.

As regards the institutional approach, the assessment for the data protection field is based on the consultation of the institutional activity of the IDP Commissioner, whilst for the AML area interviews and Focus Groups Discussion are conducted with AML stakeholders.

Specifically, in order to understand which was the level of awareness towards data protection in Albania and the approach embraced by the IDP Commissioner, we consulted the sublegal instruments issued by the latter in virtue of the Data Protection Law, as well as administrative documents produced following inspection visits conducted with regard to AML related stakeholders.

The assessment of the institutional approach on the side of AML related stakeholders is mainly based on interviews conducted with them, in order to understand their practical approach in their day-to-day activity vis-à-vis data protection rules.

Then a cross check of the data collected through documentary consultation and interviews and Focus Group Discussion followed, whereof additional conclusions as of the state of play of the balance between the two domains (i.e., AML vs. data protection) were drawn. This is reflected in details under subchapter VI.2 of this Report.

To this purpose interviews with 12 (twelve) AML related stakeholders, from both, public and private sector, are conducted. Specifically, out of these controllers, 7 (seven) interviewees were from the public sector, namely:

(i) the Albanian Financial Intelligence Unit (i.e., which did not positively reply to our request for interview, but provided a partially filled in questionnaire);

(ii) the Anti - Corruption Unit near the Prime Minister's Office;

(iii) the Prosecution Office;

(iv) the General Police Directorate;

(v) the Bank of Albania;

(vi) the National Business Center; and

(vii) the General Tax Directorate.

Private stakeholders interviewed are selected among entities that are subject to AML law in Albania; specifically, a second-tier bank operating in Albania, a non-for-profit organization, a notary public, a real estate agency and a broadcasting company.

The interviews are extended in a two months range of time, starting as from April 2021, with the last interviews being concluded in the middle of May.

After conclusion of the interviews' session, a Focus Group Discussion with AML related stakeholders followed, whereof interesting insights emerged with regard to the practical approach adopted by AML related stakeholders towards data protection rules.

It is to be emphasized that the information of Focus Group Discussion is based on the statements of the persons designated to represent each stakeholder for purpose of the interview, and no responsibility is borne by the experts as to the accuracy of the information provided by the participants in the Focus Group Discussion.

# IV. AML LEGISLATION

The AML legislation in Albania is composed of numerous instruments, varying from convention to laws and sublegal acts, which deal with the rules, terms and procedures applicable to the Obliged Entities, AFIU and other AML related authorities.

In this regard, the following instruments are to be mentioned:

(x) Council of Europe Convention on the Prevention of Terrorism;

(xi) Council of Europe Convention on Laundering, Search, Seizure and Confiscation of Pro ceeds from Crime and Financing of Terrorism;

(xii) AML Law;

(xiii) UBO Law;

(xiv) Law on Bank Accounts Registry;

(xv) Anti-Terrorism Measures Law;

(xvi) Law on Administration of Sized Assets;

(xvii) Law on International Coercive Measures in the Republic of Albania.

(xviii) Sublegal acts issued on applicability of the abovementioned instruments.

The most important acts in the context of this Report regarding of level of approximation with 4th and 5th Directives, and compliance with data protection legislation, are the ones indicated under points (iii) to (v) above.

Firstly, the AML Law having as scope the prevention of money laundering and products deriving from criminal offences, as well as the prevention of terrorism financing.

AML Law provides for the detailed rules and regulations regarding the AML surveillance, costumer due diligence (i.e., standard, simplified and enhanced one), categories of (personal) data being processed (i.e., collected, retained, transferred) for purpose of AML compliance and assurance, the categories of persons/entities being subject thereof, AML reporting obligations on the part of Obliged Entities, functions and responsibilities of AFIU, etc.

Secondly, the UBO Law that provides for establishment, functioning and administration of the UBOs Registry, as well as the registration procedure and the data to be filed by the Obliged Entities as per UBO Law.

Further, the UBO law defines the categories of UBOs data that are registered and retained in the UBO registry, the Obliged Entities, the third parties' access to UBOs data, the reporting obligations, etc. The holder of UBO registry is NBC (i.e., which holds also the Albanian Commercial Registry and Registry of Licenses, Permits and Authorizations).

Thirdly, the Law on Bank Accounts Registry, which determines the principles and rules for the establishment and functioning of the Registry of Bank Accounts, the access rights, as well as the obligation of Obliged Entities (i.e., financial institutions) for reporting the bank account data (i.e., owner, account no., IBAN, transactions, etc.) to such registry. Holder of the Registry of Bank Accounts is the GTD.

## IV.1 Legislation development

Below is shown the historical outline of the main developments related to the establishment and institutional consolidation of the AML legislation in Albania.

In May 2000, the Albanian Parliament, based on the recommendation of MONEYVAL Committee, approved the law no. 8610, 17.05.2000 "*On the prevention of money laundering*".

In November 2006, the Conventions of the Council of Europe (i) on the Prevention of Terrorism and (ii) on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and Financing of Terrorism were ratified.

In May 2008, the AML Law was approved, which entered into force on September of the same year. The purpose of this law was to approximate the Albanian legislation with the international recommendations of the FATF.

In March 2011, the first amendment to the AML Law was approved.

In June 2012, the second amendment to the AML Law was approved.

In October 2013, the Anti-Terrorism Measures Law, was approved.

In April 2017, the third amendment to the AML Law was approved;

In June 2019, the fourth amendment to the AML Law was approved.

In July 2020, the UBO Law was approved.

In December 2020, the Law on Bank Accounts Registry was approved.

As of February 2021, the draft of the fifth amendment to the AML Law is under public consultation process.

## IV.2 Cross-border cooperation in AML/CTF issues

Albanian AML legislation provides for the entitlement and, concurrently, the obligation of domestic AML authorities to cooperate with foreign AML authorities and international organizations, *inter alia*, through exchange of information and mutual legal assistance.

The cross-border cooperation is set out in different legal instruments that are directly binding to the Obliged Entities and AML authorities.

As indicated in subchapter IV.1 above, Albania has ratified the Conventions of the Council of Europe (i) on the Prevention of Terrorism and (ii) on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and Financing of Terrorism.

According to these conventions, Albania (i.e., AML authorities) shall cooperate, assist and support other countries for purpose of enhancing capacities to prevent and combat the commission of terrorist and money laundering offences. This has to be done, among the others, through assembling, analyzing and investigating, money laundering facts-related information, exchange of such information, joint efforts of a preventive character, etc.

In this context Albania cooperates with other jurisdictions through the Egmont Secure Web – "**ESW**"[185], which is the platform of cooperation put in place by Egmont Group, of which AFIU is a member of since 2003[186]. Through this is aimed at exchanging not only the AML/CTF related information between FIUs, but also the exchange and enhancement expertise on AML/CTF issues of FIUs that are members of Egmont Group.

[185] https://fiu.gov.al/international-cooperation/.
[186] https://www.egmontgroup.org/en/content/albania-general-directorate-prevention-money-laundering.

Moreover, as member of Council of Europe and as a Party to the Convention of the Council of Europe on Laundering, Search, Seizure and Confiscation of Proceeds from Crime and Financing of Terrorism, Albania is subject to evaluation on the part of the MONEYVAL and, therefore, it is under continuous process of improvement of international cooperation efforts in field of AML/CTF issues, as well as for strengthening the application of AML/CFT actions and measures, and for purpose of achieving compliance with the recommendations of FATF.

Although not among the FATF List of Countries Albania, as a country with strategic deficiencies in the AML regime, since February 2020[187], Albania has been put under increased monitoring by both, Moneyval Committee and the ICRG[188], due to its commitment to work with the FATF and MONEYVAL to strengthen the effectiveness of its AML/CFT regime and the steps undertaken towards improving its AML/CFT regime, by ensuring that supervisory authorities of non-financial businesses and professions take a risk-based approach and incorporate AML/CFT components into their inspections[189]. However further steps are required to be taken towards proper implementation of the action plan to address its strategic deficiencies[190]. Based on the relevant MONEYVAL reports, Albania reports back thereto regarding the progress made for addressing the relevant findings of respective MONEYVAL evaluation reports.

Moreover, the obligation for international cooperation is set out also under the AML Law and Anti-Terrorism Measures Law that govern specifically AML/CTF matters.

Subject to article 22 of AML Law, among the task to be accomplished by AFIU, is the exchange of information with any foreign counterpart agency, the conclusion of any agreements with the latter, submission of requests for mutual legal assistance, etc.

This is further normatively reiterated by article 9 of the Anti-Terrorism Measures Law that obliges other AML related authorities (i.e., such as the ministers of finance, interior, foreign affairs, justice, defense, the General Prosecutor, the head of State Intelligence Service, the Governor of the Bank of Albania, etc.) to exchange information and data at international level regarding the listed persons, who are suspected as involved in terrorism financing offences.

Therefore, without prejudice to the forms of exchange indicated herein above, AFIU liaises and cooperates with its international counterparts (i.e., Financial Intelligence Units – the "**FIUs**") through free exchange of information or, if this is not allowed in certain jurisdictions, through Memorandums of Understanding (the "**MoUs**"), based on which are set out the rules for cooperation and exchange of information regarding suspicious transactions issues involving money laundering and/or terrorism crimes[191].

Currently there are in place 43 MoUs with partner FIUs around the world[192].

Additionally, Albanian AML authorities and stakeholders are obliged by letter of law to address the decisions of the international organizations, where Albanian is a member of, to use the mechanism of direct freeze accounts/funds/assets of listed persons.

To this effect, AML legislation prohibits the Obliged Entities from carrying out financial transactions for persons listed by decision of the United Nations Security Council, as per the relevant international acts, conventions and/or international treaties where the Republic of Albania has adhered to, as well as obliges these entities and AML authorities to (temporarily) freeze the accounts/funds/assets of the such listed persons, directly, without preconditioned by a temporary freeze/seizure order or

187 http://www.fatf-gafi.org/countries/a-c/barbados/documents/increased-monitoring-february-2021.html,
188 Page 29 of the AFIU Annual Report for 2020.
189 http://www.fatf-gafi.org/countries/a-c/barbados/documents/increased-monitoring-february-2021.html.
190 http://www.fatf-gafi.org/countries/a-c/barbados/documents/increased-monitoring-february-2021.html.
191 https://fiu.gov.al/international-cooperation/
192 Same as footnote 7 above.

other domestic (enforcement acts) acts applying to similar interim/precautionary measure[193].

In addition to the legal provision applicable directly to AFIU and other AML authorities and stakeholders, there are also other "auxiliary" legislation provisions that deal with the international cooperation between the Albanian authorities, such as, without limitation, the State Police, General Prosecution Office, etc., aiming at combating the financial crimes (i.e., including the money laundering and terrorism financing offences).

As such one might mention the mechanisms of exchange provided under the Code of Criminal Procedure, or the one under article 24 of the law on State Police.

In this context, as of December 2013, Albania has stipulated the Agreement on Cooperation with Europol, whilst as of 2018 has ratified the Agreement on Cooperation with Eurojust (Law no. 113/2018 "On ratification of the Cooperation Agreement between the Republic of Albania and Eurojust").

Further, since 1991, Albania is a member country of Interpol.

As regards the approximation with the 4th Directive (as amended through the 5th one), it is to be noted that provisions concerning the cooperation between AFIU and foreign counterparts (i.e., FIUs) in AML/CTF issues, likewise under 50a of the Directive, are not yet fully approximated.

The fifth amendment (i.e., which is still under process of review and consultation between the stakeholders) of the AML Law addresses this accordingly.

## IV.3 Level of approximation with 4th and 5th Directives

As indicated under subchapter IV.1 above, AML Law has been amended four times so far and the fifth amendment is still undergoing the mandatory legislative route applicable in case of the approval of a law in Albania.

In this view, one might note that two out of four amendments of AML Law (i.e., namely the third and the fourth one) are enacted following the approval of the 4th Directive. Whilst one out of four amendments (i.e., the fourth one) is enacted following the approval of the 5th Directive.

It is worth mentioning that none of the four amendments to the AML Law had as purpose the (full or partial) approximation with the 4th and 5th Directive.

This is also attested by the content of the mandatory explanatory report accompanying the draft of the fourth amendment to the AML Law, where it is stated that the scope of such amendment is the approximation with FATF recommendations; not the direct approximation with the 4th and 5th Directives[194].

As such, it is clear that AML Law is not fully approximated with the foregoing directives.

Indeed, as of currently, the AML Law is approximated with 3rd Directive, which has been repealed by the 4th Directive.

The first legislative actions on approximation of the Albanian AML Legislation with 4th and 5th Directives are undertaken and (partially) concluded through UBO Law and the Law on Bank Accounts Registry.

The aim of these instruments is the approximation with the 4th and 5thDirectives[195].

In the light of the above, considering the scope of each of these laws one might conclude that the AML legislation in Albanian is only partly approximated with *acquis communautaire* in the field of AML.

[193] Article 10 of AML Law, in conjunction with article 10/1 of Anti-Terrorism Measures Law.
[194] Explanatory report on the fourth amendment, point V pg. 3.
[195] Explanatory report on the UBO Law, point V, and Explanatory report on the Law on Bank Accounts Registry, point V.

Moreover, the partial state of approximation is also confirmed by the (preliminary) mandatory explanatory report accompanying the draft of the fifth amendment to the AML Law, which aims at bringing the Albanian legislation in full compliance with the 4th and 5th Directives[196].

Pursuant to the information reflected in the explanatory report accompanying the draft of the fifth amendment to the AML law, the Republic of Albania has committed itself on the full approximation of the AML law with the *acquis communautaire* by means of different instruments. As such, this commitment is first reflected in the Association and Stabilization Agreement entered into between the Republic of Albania and the EU, as ratified upon law no. 9590, dated 27.07.2006.

Further, as indicated in the 4th objective of the Joint Action Plan on Anti-Terrorism Measures for the Western Balkans stipulated between Western Balkans and EU representatives, the Republic of Albania has committed to conclude the full approximation of its AML legislation with *acquis communautaire* within 2020 – 2021.

Full approximation of the Albanian AML legislation with the *acquis communautaire* is currently a request addressed by the EU, which has solicited the full approximation to be completed within October 2021.[197]

The proposed fifth amendment to the AML Law provides, *inter alia*, for the unification of the terminology, the enlarging and clarification of the categories of reporting entities and the mode of reporting at AFIU, in accordance with provisions of the 4th and 5th Directives.

Nonetheless, as it is shown in the ToC, even if the fifth amendment to AML Laws will be approved by the Albanian Parliament, as per the current content thereof, no full compliance with the 4th and 5th Directives would be achieved.

## IV.4 What is still missing to full compliance?

The literal answer to this query is tabularly given in the ToC.

In any case, the answer to this query has assessed the material compliance of the domestic legal instruments vis-à-vis AML *acquis*; not the implementation in practice of the material provisions of AML legislation by the competent authorities and/or obliged entities.

Thus – as it is shown below in this Report – the material compliance, does not necessarily mean a compliant behavior on the part of the competent authorities and/or obliged entities vis-à-vis their legal (material) obligations.

Below are listed, as way of example, but not exhaustively, some the material discrepancies between the Albanian AML Legislation and the 4th and 5th Directives (i.e., supposing hereby that the fifth amendment to the AML Law would be approved as per its current content):

(i) The Albanian AML Legislation does not provide for the existence of the concept/instrument of the "*self-regulatory body*" (i.e., unlike the 4th Directive (as amended by the 5th one), which deals therewith, *inter alia*, in article 3(5) thereof);

(ii) The Albanian AML legislation does not provide a narrow definition of the "*correspondent relationship*" (i.e., unlike the 4th Directive (as amended by the 5th one), which deals therewith, *inter alia*, in article 3(8) thereof);

(iii) The Albanian AML legislation does not contain any thresholds for the derogation of AML due diligence (i.e., unlike the 4th Directive (as amended by the 5th one), which deals therewith in article 12 thereof);

[196] Explanatory report on the fifth amendment, point I.
[197] Explanatory report on the fifth amendment, point III, page 2.

(iv) The Albanian AML legislation provides only for the exemption of the legal professionals from the reporting obligation regarding the information obtained from their customers, *inter alia*, in the ambit of court representation; the notary publics are not exempted from such obligation, whilst auditors, external accountants and tax advisors are not mentioned at all in this context (i.e., unlike the 4th Directive (as amended by the 5th one), which deals therewith in articles 14(5) and 34(2) thereof);

(v) The Albanian AML legislation does not provide for the exclusion of the outsourcing or agency relationships from being considered as "third parties", on which the obliged entities might rely on when performing customer due diligence (i.e., unlike the 4th Directive, which deals therewith in articles 29 thereof);

(vi) The Albanian AML legislation provides for the case of limitation of access to the UBO registry only for persons that require access thereto based on legitimate interest, whilst the obliged entities are not subject to such limitation (i.e., unlike the 4th Directive, which deals therewith in articles 30(9), 31(4) and 31(7) thereof);

(vii) The Albanian AML legislation does not specifically provide for entitlement of the individuals (including employees) who are exposed to, *inter alia*, retaliatory, hostile, or discriminatory actions for reporting suspicions of money laundering, to AFIU, to present a complaint in a safe manner to the respective competent authorities (i.e., unlike the 4th Directive (as amended by the 5th one), which deals therewith in articles 38).

It is to be mentioned that this kind of entitlement is provided for under the whistleblowing legislation, that, indeed, deals with the reporting of corruption practices, which not necessarily relate to AML offences;

(viii) The Albanian AML legislation does not provide for the derogation of the prohibition of disclosure, in cases of exchange of AML related information, *inter alia*, between the credit/finance institutions and their branches and subsidiaries in other countries (i.e., unlike the 4th Directive (as amended by the 5th one), which deals therewith in articles 39(3)/(5)/(6) thereof);

(ix) The Albanian AML legislation provides for different data retention periods comparing to that of article 40 of the 4th Directive (as amended by the 5th one)[198];

(x) The Albanian AML legislation does not provide for a clear catalogue of provisions dealing with the personal data protection obligations (i.e., unlike the 4th Directive (as mended by the 5th one), which deals therewith Chapter V thereof);

(xi) The Albanian legislation does not deal with the actions that the competent authority should take in case of warnings served by the obliged entities regarding the difficulties/obstacles faced by the latter for implementing their information sharing procedures and policies in other jurisdictions where they are present through their branches and/or subsidiaries (i.e., unlike the 4th Directive (as amended by the 5th one), which deals therewith under article 45(5) thereof);

From the ToC, it is observed that there are 139 out of 216 provisions which are compatible with the Directive, 61 out of 216 are partially compatible, and 15 provisions out of 216 which are not compatible.

[198] The related analysis in this regard is to be found in Chapter V of this Report.

Mathematically speaking the AML legislation is **65 %** compatible, **28%** partially compatible, and **7%** not compatible with the Directive.

Considering the fifth amendment, which is currently under legislative process, 28 out of 61 partially compatible provisions would turn compatible if the amendments would be approved as per the current content.

Some of the provisions which would turn compatible if the draft of the fifth amendment would be approved by the Parliament (i.e., supposing that the fifth amendment to the AML Law would be approved as per its current content) are listed below:

(i) Provisions dealing with the categories of entities/persons being subject to the AML law indicated under article 2 of the Directive;

(ii) Definitions which will apply to the AML law as indicated under articles 3.2, 3.9, 3.11., 3.12, 3.17, and 3.19 of the of the Directive

(iii) Provisions which determine risk factors to be taken into consideration by obliged entities when determining the preventive measures to be put in place in line with article 13.5 of the Directive

(iv) Provisions dealing with due diligence requirements applicable to life or other investment related insurance policies customers or beneficiaries in line with article 13.5 of the Directive

(v) Provision dealing with due diligence requirements applicable on beneficiaries of trust or other legal arrangements as per article 13.6 of the Directive

(vi) Provisions dealing with enhanced due diligence measures required in connection with business relationships or transactions with high risks countries as per article 18a, 18a.2, 18a.3 and 18a.4 of the Directive

(vii) Provisions dealing with the right of the competent authority to refuse cooperation or exchange of information based on objective grounds in line with article 32.5 of the Directive

(viii) Provisions dealing with the right of the Albanian finance intelligence unit to obtain feedback from other competent authorities on the use of the information provided by such unit and on the outcome of investigations performed based on such information

(ix) Provisions dealing with the obligation of obliged entities indicated under article 45.9 of the Directive to appoint a contact person who will be responsible to ensure compliance with AML/CFT rules

(x) Provisions dealing with the obligation of obliged entities to undertake proportionate measures so as to permit their employees in connection with AML/CFT and data protection rules as indicated under article 46 of the Directive

(xi) Provisions dealing with the appropriate measures taken to prevent criminals from possessing, holding a management function or being the beneficial owners of obliged entities indicated under article 47.3 of the Directive

(xii) Provisions dealing with the measures that should be taken in order to ensure adequate supervision of the obliged entities either by the Albanian financial intelligence unit or by their respective supervising authorities in line with article 48.1a of the Directive

(xiii) Provisions dealing with cooperation between counterpart competent authorities in the field of prevention of money laundering and countering financing of terrorism as per article 50a of the Directive.

Generally, the not compatible provisions remain such even with the amendments proposed (supposing that these amendments would be approved as per their current content) with the exception of the definition regarding family members of the politically exposed persons which is addressed under the fifth amendment to the AML law and would turn therefore compatible. Further, the one dealing with the grounds for refusal of a competent authority to exchange information with foreign counterparts would turn into partially compatible if the amendments would be approved as per the current content.

# V. DATA PROTECTION LEGISLATION

The right to data protection of a citizen (i.e., data subject) is explicitly provided for under article 35 of the Albanian Constitution, where it is unequivocally stated that the processing of personal data is based on law and/or consent of the data subjects.

According to this constitutional provision, the processing of personal data (i.e., their collection, use and public disclosure) is done upon the [informed] consent of the data subject, unless otherwise provided for by [specific] letter of law.

Save for and based on the above, the main important piece of legislation that regulates the protection and processing of the personal data within the territory of the Republic of Albania is the Data Protection Law, along with sublegal acts issued by the IDP Commissioner, which is the competent authority that monitors and supervises the compliance of data controllers and/or data processors with the legislation in force.

The provisions of the Data Protection Law apply to the processing, carried out through automatic means, or through other means, of personal data stored in a filing system, or which are intended to be part of a filing system.

Subject to such law are considered, *inter alia*, all public and private controllers of the Republic of Albania. Thus, subject thereto is also, respectively, AFIU, NBC (i.e., holder of UBOs Registry) and GTD (holder of the Registry of Bank Accounts), as well as the Obliged Entities of AML legislation.

For purpose of compliance with the applicable legislation on personal data, any data controller/ processor should act in compliance with the principles laid down under article 5 of the Data Protection Law. Such principles include as follows:

(i) '*Lawfulness and fairness*', which means that the protection of personal data should be based on a fair and lawful processing;

(ii) '*Purpose limitation*', which means the collection of personal data for specific purposes, being clearly determined and eligible, as well as on the (further) processing in compliance with such purposes;

(iii) '*Data minimization'*, which means adequacy/sufficiency of personal data, which should relate to the purpose of their processing and not be excessive in relation to such processing purpose;

(iv) '*Accuracy*', which means that the personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to erase or rectify any inaccurate or incomplete data, having regard to the purposes for which they are collected or for which they are further processed;

(v) '*Storage limitation*', which means that personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are collected or further processed;

(vi) '*Accountability*', which means that the controller shall be responsible for, and be able to demonstrate compliance with points (a) to (e) above.

In addition, in order for the processing of personal data to be considered lawful, according to article 6 of the Data Protection Law, it should be carried out only in the following cases:

(a) If the data subject has granted his/her consent on personal data processing;

(b) If the personal data processing is substantial for purpose of fulfilment of a contract, entered into by the data subject, or for purpose of discussions or amendments to a project/contract upon proposal of the data subject;

(c) For protecting the vital interest of the data subject;

(d) For fulfilment of a legal obligation of the data controller;

(e) For the performance of a legal task bearing public interest or exercising of an authority of the data controller or of a third party, to which the personal data have been disclosed;

(f) If the personal data processing is substantial for protection of legitimate interest of the data controller, data receiver or other interested persons.

A special treatment is reserved to the processing of sensitive data, which comprise any information related to a natural personal with regard to his/her racial or ethnic origin, political opinion, the membership in trade union, philosophical belief or religion, criminal background, as well as data related to health and sexual life (i.e., article 7).

The processing of sensitive data might take place, *inter alia*, if the data subject has granted his/her written consent of the data subject, if it is in the vital interest of the latter or of another person (where the data subject is physically or mentally incapable of giving the consent), if it is authorized by the competent authority for reasons of public interest, if it relates to personal data manifestly made public by the data subject or is necessary for exercise or defense of a legal claim, if it is required for purpose of preventive medicine, healthcare, management of heath care and for purpose of use on the part of the medicine personnel (who is obliged to preserve confidentiality), if it is necessary for purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and social security and social protection law.

Moreover, the data controllers are obliged to address the catalogue of rights of the data subjects as set out under Chapter IV of the Data Protection Law, such as the right to access to their personal data, right to seek blocking, rectification and deletion of their personal data, right not to be subject to automated decision-making, right to object to processing of their personal data, right to object to direct marketing and right to file complaint.

In this view, the data controllers are obliged to inform the data subject on the relevant processing activities and features; with few exemptions (i.e., as per article 18 thereof).

Further, the data controllers are obliged to notify the IDP Commissioner before starting the data processing activities, as well as on any changes of these activities whenever they happen (i.e., as per article 21 thereof).

The IDP Commissioner has dedicated a special focus to the technical and organizational measures that the controllers should take in order to guarantee the security and confidentiality of personal data, as per articles 27 and 28 of the Data Protection Law, as well as the obligations of the controllers vis-à-vis their processors, as per article 20 of such law.

Among the sublegal acts of the IDP Commissioner that put a distinct emphasis to the obligations of the controller one might mention Instruction no. 19, Instruction no. 22, Instruction no. 47 and Instruction no. 48.

It is to be noted that, in virtue of Instruction no. 22 (i.e., applicable to small data controllers) and Instruction no. 47 (i.e., applicable to large data controllers), any data controller is obliged to appoint a Data Protection Officer (DPO).

Save for the above, apart for the monitoring and supervising of compliance with personal data protection on the part of the controllers, one of the competences of the IDP Commissioner is the provision of opinions for different project-acts (i.e. including, but not limited to, draft laws) of public controllers, in the light of the provisions of the legislation on personal data protection, as well as the publication of recommendations regarding the proper implementation of the requisites of the Data Protection Law by (public) controllers (i.e. as per point 1 of article 31 of the Data Protection Law).

On the other hand, this competence of the IDP Commissioner corresponds to an (institutional) obligation for public controllers for addressing the IDP Commissioner, in order to obtain the necessary opinions of the latter for purpose of assessing *ex ante* the level of compliance of the relevant project-acts with the legislation on personal data protection.

## V.1 Legislation development

The following represents a historical outline of the main developments related to the enactment of the data protection legislation in Albania.

In July 1996, the European Convention on Human Rights was ratified (i.e., including article 8 thereof – Right to respect for private and family life).

In October 1998, the Constitution of the Republic of Albania (which includes the right of personal data protection under its catalogue of human rights – article 35).

In July 1999, the law no. 8517, dated 22.7.1999 "*On personal data protection*" was amended.
In April 2004, the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, were approved.
In March 2008, the Data Protection Law is approved (i.e., repealing the former one). Since then, this instrument has been amended only twice. The first amendment was approved in April 2021, and the second amendment in September 2014.
A large contribution in the development of the legislation of personal data protection has given the IDP Commissioner, who has been very active in the enactment process of sublegal acts (i.e., having general scope and/or dealing specifically with different areas of the law).
Statistically speaking, the IDP Commissioner, throughout 13 years of its institutional existence, has issued more than 60 sublegal acts (i.e., decisions, instructions, unified recommendations) that have paved the way for enabling the contractor an as easy as possible way for aligning and complying with the provisions of the legislation in force on personal data protection.

## V.2 Level of approximation with *aquis communautaire*

The Data Protection Law is fully approximated with Directive 95/46/EC.

On the other hand, the IDP Commissioner has already "transposed", in virtue of its sublegal acts (i.e., instructions), several novelties introduced by GDPR, such as the mandatory position and the role of the data protection officer, the data impact assessment, the information security policy, the appointment of the DPO, the certification mechanism, etc.

Moreover, since September 2020, the IDP Commissioner is in process of preparation the draft law aiming at fully approximating the Albanian data protection legislation with GDPR, benefiting from a twinning project, financed by the Delegation of the European Commission in Albania and technically assisted by the consortium of the Italian supervisory authority Ludwig Boltzmann Institute for Human Rights, Austria.

Although there is no formal parliamentary instrument in place that certifies the level of approximation with GDPR, considering the “flood” of sublegal acts of the IDP Commissioner, one might conclude that there is, already, a concrete (however partial) GDPR approximation reality in Albania.

# VI. AML LEGISLATION VIS-À-VIS DATA PROTECTION LEGISLATION

For purpose of assessing the extent to which the provisions of the AML Legislation account to the principles and criteria on the lawfulness of processing of personal data, it should be distinguished the formal material situation (i.e., systematic compliance between the provisions of each legislation) from the institutional behavior of the public bodies/authorities and Obliged Entities – which process personal data in the ambit of AML legislation – vis-à-vis the Data Protection Law.

Based on the constitutional approach that the processing of personal data (i.e., including the eventual obligation of data subjects to disclose them) is subject to either [specific] law provisions or to the [informed] consent of the data subject, one might reasonably say that – in general – the provisions of the AML legislation rely on those of Data Protection Law.

Nonetheless, from a conservative data protection perspective, there are still some "hot spots" that would trigger legal uncertainty to the stakeholders involved in the mandatory compliance perimeter of AML legislation, *inter alia*, with regard to their obligations vis-à-vis the rights of data subject[199].

Moreover, as indicated under letter (x) of subchapter IV.4 of this Report, the Albanian AML legislation does not fully address the data protection concerns of the 4th and 5th Directive.

On the other hand, despite the normative compliance assumption between such laws (i.e., based on systematic interpretation of the law provisions), there have been several cases when the *de facto* requirements that AFIU and/or Obliged Entities have imposed on the data subjects, in virtue of an extended interpretation of the AML Law, have violated the provisions of the Data Protection Law.

In this view, it is to be mentioned, for example, the requirement of AFIU (prior to entry into force of the UBO Law) that all Obliged Entities should collect the ID cards of UBOs, whilst such requirement was not explicitly provided for under the AML Law.

As mentioned above, the processing of personal data is to be based on [specific] law provisions or consent of the data subjects. Under the circumstances that the AML Law did not require the ID of the UBOs, the only lawful criteria available for processing such information was the [informed] consent of the UBOs themselves.

Obviously, not in all cases the Obliged Entities succeeded to obtain the consent of UBOs, bring themselves into a position of procuring such IDs through other ways (i.e., constituting herewith a breach of Data Protection Law), in order to avoid the (disputable) fines applied by AFIU in case of lack of such ID cards in the relevant customer files of the reporting entities.

The above example shows the difference between the normative regulation of AML Law and the institutional behavior of AML enforcing bodies, which, upon entry into force of UBO Law, is reduced but not yet overcome[200].

## VI.1 Material compliance between AML and data protection legislation

From the review of the provisions of the AML Law, the following issues have data protection insecurities inherent to them:

(i) The data retention period as per AML Law.

According to article 16 of the AML Law, the Obliged Entities must retain for a period of 5 years, *inter alia*, the documents obtained in the ambit of standard and enhanced due diligence, the registries related to data, reporting and documentation for domestic and cross border transactions, etc.

[199] See below in subchapter VI.1.

[200] See below in point (iv) of subchapter VI.1.

However, the same provision states that, upon request of AFIU, such documentation/ information must be retained for more than 5 years, constituting herewith an open-ended retention term.

It is to be noted that, according to article 22(gj) of the AML Law, AFIU itself may retain the documentation/information [received in the ambit of its legal activity] for a term of 10 years from receipt date[201].

This open-ended data retention term creates huge legal uncertainty for the Obliged Entities, when addressing the mandatory compliance matters with Data Protection Law.

In this view, the Obliged Entities would not be in the position to accurately define the data retention term when addressing the information obligations toward their clients (i.e., data subjects).

The relationship between an Obliged Entity and a data subject is based on the contractual relationship that they agree to conclude based on their mutual will. Therefore, in the first place, the processing of personal data by an Obliged Entity is based on the [informed] consent of the data subject to conclude the agreement and, thus, accept the processing of his/her personal data for purpose of such contractual relationship and for such other legally mandatory purposes (i.e., AML purposes) that apply to the existence of such contractual relationship.

At this point, the Obliged Entity would be obliged to inform the data subject about the data retention period, which, in virtue of the open-ended retention term provided for under article 16 of AML Law is barely predictable.

Furthermore, the right of AFIU to seek from Obliged Entities store the data for longer (i.e., undefined) retention periods, even in excess to the retention period appliable to AFIU itself, constitutes a normative nonsense that, again, would contribute to very detrimental consequences to the Obliged Entities, not only from the legal point of view, but also from cost perspective.

Thus, in order to address the information obligations toward data subjects, the Obliged Entities would be obliged to perform repetitive *ex post* information campaigns, whenever an extension of the data retention period would be required by AFIU.

Additionally, the cost for taking and maintaining the mandatory technical and organizational measures (i.e., including, the applicable information security management system) would be continuously augmented.

On the other hand, for data subjects themselves it becomes uncertain for how long their data would be stored by the Obliged Entities, with whom they opted (i.e., were not obliged) for entering into contractual relationships, constituting herewith also huge concerns regarding their privacy.

Last but not least, what draws the most one's attention is the fact that, according to the entitlement reserved to AFIU as per article 16 of AML Law, this body has a vast discretional room for purpose of deciding the duration of the retention period of the data processed by Obliged Entities.

Thus, apart for the risk of arbitrary behavior on the part of AFIU inherent to this provision, it is also clearly incompliant with the provisions of 4th and 5th Directives in relation to this subject matter.

[201] The same 10 years term applies also to NBC (i.e., regarding the data stored with the UBOs Registry) and to GTD (i.e., regarding the data stored with the Registry of Bank Accounts).

According to article 40(1) of the 4th Directive (as amended by the 5th one), upon expiry of 5 years retention term, the Obliged Entities should delete the personal data, unless otherwise provided for by national law, which shall determine the circumstances that would oblige the said entities to further retain data.

In addition, according to the foregoing *acquis* provision, the further retention of personal data might be carried out only for other 5 years, based on a thorough assessment of the necessity and proportionality of such further retention and consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. As it may be noted, the spirit of the 4th and 5th Directive is that the further retention is not mandatory, but rather decided on case-by-case basis following a thorough assessment as to the necessity which determine such further retention.

The AML Law, *prima facie*, imposes no obligation to AFIU for reasoning the necessity and proportionality of further retention periods of personal data, when ordering the Obliged Entities to do so.

(ii) The different data retention terms throughout different instruments of AML legislation.

Article 16 of AML Law appears to conflict with article 7(2) of the Law on Bank Accounts Registry that obliges, *inter alia*, the entities entitled to obtain information from the Registry of Bank Accounts (i.e., comprising, *inter alia*, the financial institutions, which are Obliged Entities as per AML Law) to retain that information (i.e., including the personal data inherent thereto) for a period of 10 years following the receipt date.

In this view, the conflict between the abovementioned provisions of AML legislation, exposes the relevant Obliged Entities, again, toward legal uncertainties. This normative conflict constitutes an impediment for the Obliged Entities for complying with the storage limitation principle as set out under article 5 of the Data Protection Law.

As such, the concerned Obliged Entities have to accurately identify and segregate the data that are to be retained as per the 5 years retention term set out under article 16 of AML Law and the ones that should be stored for the 10 years mandatory term of the Law on Bank Accounts. Otherwise, the *en bloc* storage of the data for the latter term might be construed as breach of storage limitation principle.

Moreover, it is worth mentioning that, according to article 27 of AML Law, the data retention period in breach of article 16 is subject to fines up to ALL 8,000,000 (approx. EUR 65,000).

On the other hand, the open-ended retention term of article 16 of AML Law appears to grant to AFIU the right to derogate provisions of article 7(2) of the Law on Bank Accounts, when requesting to an Obliged Entity to further retain the data processed for AML compliance purpose for a term that exceeds the 10 years term of article 7(2) of the Law on Bank Accounts.

(iii) Article 24(2) of the AML Law.

According to this provision, the supervisory authorities listed under article 24(1) of the AML Law[202] are entitled, for purpose of this law and irrespective of the provisions of other laws (i.e., including herewith, the law on personal data protection), to seek from the Obliged Entities under their mandatory supervision any sort of information and documentation that is related to the compliance of the latter with the provisions of the AML Law.

On the other hand, according to article 22(b) of the AML Law, the AFIU is also entitled to

[202] As supervisory authorities are listed the (i) Bank of Albania (ii) Financial Supervisory Authority (iii) some ministries and other supervisory bodies of different Obliged Entities, (iv) Albanian Bar Association (for lawyers) and (v) the Ministry of Justice (for notaries).

have direct access to the information processed by public institutions/authorities and Obliged Entities. However, subject to the same provision, the processing of personal data by AFIU has to be performed in accordance with the rules of the applicable data protection legislation.

To this effect, *prima facie*, appears that the AML Law contains a double standard as regards the access to personal data.

Surprisingly, the AML Law derogates the eventual legal burdens and restrictions that other laws would contain for the access to the information to the benefit of supervisory authorities, but binds AFIU itself, *in expressis verbis*, to the rules of the applicable data protection legislation in relation to this matter. It is to be noted that the supervisory authorities are obliged to report to AFIU.

This twisted approach of the AML Law concerning the [fully] unrestricted access of the supervisory authorities to the information of the relevant Obliged Entities creates confusion to the latter as regards the fulfillment of their obligations toward the data protection legislation.

Paradoxically, the AML Law does not set out any retention term for such information, which the supervisory authorities would be bound to and, subsequently, for the deletion of the information upon expiry thereof.

What further emerges from such provision is that by letter of law no reference to necessity or proportionality test is made in connection with the access that supervisory authorities are entitled to have on information and/or documentation kept by Obliged Entities. Apparently, the supervisory authorities may ask to Obliged Entities access and provision or any kind of information and/or documentation for purposes of identifying compliance with the obligations arising out of AML Law.

This approach, which seems be-folded (i.e., applicable either in the material and the institutional aspect) is in conflict with one of the main principles of personal data protection, the "data minimization principle" sanctioned under article 5 of the Data Protection Law[203].

(iv) The lack of data subject related provisions in the AML Law.

From the optic of a data subject, the provisions of the AML Law would imply that their personal data are going to be processed at three different levels (composed of many horizontal actors at each level) for the same purpose (i.e., AML compliance).

As such, in case of a bank transaction, the personal data of a data subject are going to be processed (i.e., *inter alia* collected, retained, transmitted/transferred, combined, etc.) from, at least two banks, a supervisory authority (i.e., Bank of Albania), the NBC as holder of the UBOs Registry, GTD as holder of the Bank Accounts Registry, and by AFIU.

Moreover, this information might be further accessed by other law enforcement authorities, as well as circulated between the involved banks and, eventually, their branches/subsidiaries, etc.

This complex architecture of data flow would imply the necessity that a data subject is thoroughly informed, *ex ante*, on the route that their data would be pursuing, if he/she accepts to perform a certain transaction that would be subject to (standard and/or enhanced due diligence) on the part of the involved AML stakeholders.

However, AML Law, being the most important instrument in relation to the prevention of money laundering, does not provide for any provision that obliges the Obliged Entities to thoroughly and as extensively as possible informing the data subjects in relation to the processing of their personal for AML compliance purposes.

[203] See above in chapter V of the Report, page 17.

It is worth mentioning that only article 11(3) of the Law on Bank Accounts Registry provides for the obligation of the financial institutions to inform the data subject as per the provisions of the data protection legislation.

The lack of such provision in the AML Law (i.e., whilst present in the Law on Bank Accounts Registry) demonstrates again the partial alignment of the Albanian AML Legislation with the 4th and 5th Directives.

According to article 41(3) of the 4th Directive, the Obliged Entities shall provide new clients with the information required pursuant to Article 10 of Directive 95/46/EC (i.e., which corresponds with article 18 of the Data Protection Law) before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of Obliged Entities under the 4th Directive to process personal data for the purposes of the prevention of money laundering and terrorist financing as referred to in Article 1 thereof.

(v) Lack of harmonized approach toward data protection legislation throughout the AML legislation.

Points (i) to (iv) above demonstrate the lack of a harmonized approach of the Albanian AML legislation toward personal data protection one.

The abovementioned discrepancies and conflicts between the norms of the same sector have adverse effects on legal certainty needed by the AML stakeholders and, especially, by the data subjects.

Chapter V of the 4th Directive (as amended by the 5th one), indeed, provides for the necessity that any Member State should contain a clear catalogue of provision that deal with the personal data protection matters.

This topic becomes of paramount importance, particularly, when defining the perimeter of restrictions/derogations of the rights of data subject (i.e., including, but not limited to, the right to access, the right to seek blocking and deletion of own personal data) in relation to the processing of their personal data for AML purposes.

The elimination of such discrepancy, and the full alignment with the provision of the 4th and 5th Directives concerning the personal data matters, would bring more legal certainty for all AML stakeholders and data subjects (i.e., customers, UBOs, etc.).

## VI. 2 Institutional approach

The institutional approach and behavior of AML stakeholders (i.e., AFIU, NBC, GTD and Obliged Entities) is to be analyzed, both, from the monitoring/supporting and supervising perspective of the Data Protection Law.

As mentioned in Chapter V above, the IDP Commissioner is the responsible data protection supervisory authority in Albania.

Throughout its lifetime until now, the IDP Commissioner has embraced a proactive approach as regards the effort for assuring legal certainty to all data controllers in the country through the enactment of numerous sublegal acts, as well as through publication of its specific or unified recommendations, decisions or orders in conclusion to the investigation proceedings that it has carried out *ex officio* and/or based on complaints submitted by the data subjects.

Below is given a general overview of the activity of the IDP Commissioner vis-à-vis the AML legislations, AFIU, NBC, GTD and Obliged Entities, in the light of the data protection legislation, based on the information obtained near this authority for purpose of this Report, as well as through the information collected in the ambit of the interviews conducted with the local stakeholders and the focus group discussions.

(i) Opinions of the IDP Commissioner in the ambit of novelties of AML legislation.

According to article 31 (1/a) of the Data Protection Law, the IDP Commissioner is responsible for providing its opinions regarding the drafts of legal and sublegal acts relating to personal data, as well as regarding the projects that are to be implemented by the public controllers severally or in cooperation with other controllers/processors, which imply persona data processing.

This responsibility, anchored in the foregoing provision of Data Protection Law, is to be construed also as an obligation of the relevant public controllers to seek, *ex ante*, the opinion of the IDP Commissioner regarding the drafts of laws/sublegal acts and the projects that are to be implemented by them, implying also personal data processing.

For sake of clarity, it is to be emphasized that, according to the Albanian legislation, the legal initiative for the enactment of new or amending laws (and/or sublegal acts) pertains formally to the ministry that covers the relevant area/sectors that is to be subject of legal novelties. As regards AML sector, this formal initiative pertains to the Ministry of Finance, which is the authority where AFIU has direct reporting obligations, as per AML Law.

However, in practice, the relevant authorities who are subject to such instruments are the *de facto* authors of the first drafts thereof.

Having said the above, albeit of the legal obligation for obtaining the opinion of the IDP Commissioner for the compliance of the AML (i.e., legal and/or sublegal) acts, in many cases it is observed that the relevant AML have not always complied with such a requirement.

In this view, neither of the enacted amendments to the AML Law, nor the current draft of the fifth amendment thereof, have been submitted to the IDP Commissioner for delivering its *ex ante* opinion, from the data protection perspective, in relation to these acts.

As such, as regards the AML Law, the IDP Commissioner has been put before a *fait accompli*, without having ever had the possibility to provide its opinion in this regard, as set out by article 31(1/a) of the Data Protection Law.

On the other hand, it results that the IDP Commissioner has provided its *ex ante* opinions regarding the UBO Law[204] and the Law on Bank Accounts Registry[205].

In specific terms, from the written correspondence of the IDP Commissioner with the Ministry of Finance, in relation to assessment of the compliance of the first draft of UBO Law with the Data Protection Law, the following interventions have been proposed by the IDP Commissioner:

a. The introduction of a new provision following point 5 of article 4 of the draft of UBO Law with the following content:

"*The Registry of Ultimate Beneficiaries is established in a way that guarantees the data*

[204] Letter of the Commissioner no. 758/1 prot., dated 08.07.2020.
[205] Letter of the Commissioner no. 1107 prot., dated 28.09.2020.

*security measures, the principles of data minimization and proportionality, in relation to the processing of personal data, in accordance with the legislation on personal data protection.*";

b. The introduction of a new provision following point 6 of article 7 of the draft of UBO Law with the following content:

"*The Ultimate Beneficiaries, in the quality of data subjects, shall be informed for the subjects that access their data as per point 5 of this article.*";

c. The introduction of a new provision following point 8 of article 7 of the draft of UBO Law with the following content:

"*Any action carried out with the registry, in relation to the access, changes, rectifications, dissemination of data, etc., must leave traces for purpose of guaranteeing the security and confidentiality of the personal data.*".

In conclusion to its opinion, the IDP Commissioner, in its correspondence with the Ministry of Finance, states that upon inclusion of the above provisions the draft of UBO Law might be considered as compliant with personal data protection legislation.

It is to be noted that, at the final stage, only one out of three proposal of the IDP Commissioner (i.e., namely, point "a" above) has been included in the UBO Law.

Obviously, in the light of the above, one might conclude that, from the data protection perspective, the current UBO Law does not fully address the concerns of the Data Protection Law.

A similar situation is faced also in relation to the opinion given by IDP Commissioner regarding the compliance of the draft Law on Bank Accountings Registry with Data Protection Law.

According to the formal correspondence of the Commissioner with the Ministry of Finance in relation to the draft of this draft law, the following interventions were proposed by the IDP Commissioner:

1. The second sentence of point 2 of article 6 of the draft law be amended as follows:

   "*The system*[206] *is created, administered and maintained, in accordance with the principles, criteria, as well as the applicable technical-organizational measures applicable for guaranteeing and management of the information security, as provided for under the provisions of the legislation on personal data protection.*"

   It is to be emphasized that this proposal was based on the Resolution of the Albanian Parliament, dated 21.05.2020, which requires from the IDP Commissioner the supervision of the processing of personal data through Information and Communication Technology (ICT) systems[207];

2. It is proposed that the 10 years retention term set out under point 1 of article 11 of the draft law, should be amended in accordance with article 40 of the 4th Directive (as amended through the 5th one), which provides for a 5 years term, extendable only once for other 5 years.

   To such an end, the IDP Commissioner highlights that – same as in the 4th Directive – the further retention of personal data (for an additional term of 5 years) should be preceded

[206] It refers the ICT system on which the Registry of Bank Accounts had to rely.
[207] See the relevant remarks in point (ii) below.

by an assessment of the needs and proportionality inherent to such an extension of the retention term.

Thus, the IDP Commissioner proposed the amendment to point 1 of article 11 of the draft law, as per the following wording:

*"The information recorded in the Registry is fully stored for a period of 5 years following the closure of the bank account or safe-deposit boxes. The personal data may be retained for further 5 additional years, if, from the assessment performed by competent authorities, it results that the additional data retention term is necessary and proportional to the accomplishment of the scope of the law as provided for under article 2 thereof. […]."*

It is worth mentioning that earlier, in case of UBO Law, the IDP Commissioner has not provided any arguments against the 10 years period provided for thereunder[208].

Therefore, the opinion of the IDP Commissioner on the provisions of the draft of the Law on Bank Accounts Registry, whereby it makes direct reference to the retention terms of 4th and 5th Directives, might be construed also as complementing the opinion granted earlier by this authority (i.e., to the Ministry of Finance) in relation to the draft of UBO Law;

3. Point 2 of article 11 be amended as follows:

"*The processing of personal data, as well as the information of the data subject, on the part of the financial institutions, is carried out as per the rules set out under the applicable legislation on personal data protection*".

Whilst proposing this amendment, the IDP Commissioner, in its correspondence with the Ministry of Finance, makes direct reference article 41(3) of the 4th Directive.

In conclusion, again, only one out of three proposal of the IDP Commissioner (i.e., namely, point "3" above) has been included in the Law on Registry of Bank Accounts.

Therefore, from the qualitative point of view, one might deduce that, according to the IDP Commissioner, the level of approximation of the Law on Registry of Bank Accounts with the data protection legislation, and with the provisions to the 4th and 5th Directives dealing with this subject matter, is only partial.

(ii) IDP Commissioner vs. AFIU, NBC and GTD.

As indicated earlier in this Report, the provisions of the Data Protection Law apply to the personal data processing activities of AFIU, NBC and GTD. These authorities fall under the monitoring and supervisory responsibilities of the IDP Commissioner, in accordance with article 29 *et. seqq.* of the Data Protection Law.

Therefore, in the ambit of its supervising powers, and as per the Resolution of the Parliament, dated 21.05.2020 (hereinafter, the "**Parliamentary Resolution**"), the IDP Commissioner has carried out in the last quarter of 2020 inspecting visits to AFIU (i.e., the responsible authority as per AML Law), NBC (i.e., holder of the UBOs registry), GTD (i.e., holder Registry of Bank Accounts).

For purpose of accomplishing the tasks imposed by the Parliamentary Resolution, for the year 2020, the IDP Commissioner has inspected 12 public authorities, for purpose of supervising the level of compliance with the personal data protection and, especially, by putting emphasis to the information security measures taken by either authority subject to the relevant inspection visit.

[208] Article 9(2) of the UBO Law.

In the outcome of this investigation procedure, the IDP Commissioner has drawn up a special report[209], which has been submitted to the Albanian Parliament.

This report contains the findings and recommendations that the investigated authorities should take into account for purpose of assuring compliance with personal data protection legislation and, especially, for rigorously accounting to the mandatory principles, criteria and standards of such legislation for guaranteeing the security and confidentiality of the personal data that they process in the ambit of their activity [as controllers].

From the review of the said report of the IDP Commissioner, one might easily observe that these public controllers have insufficiencies as regards the establishment, use and administration of information security management system, especially as regards, *inter alia*, the meeting of the security measures that are accountable through standards of data confidentiality, integrity, availability and credibility.

Below is shown a summary of the IDP Commissioner's findings for AFIU, NBC and GTD:

a. *Findings regarding AFIU[210]*:

IDP Commissioner, in the ambit of, *inter alia*, the identification of processing activities and technical and organizational measures for guaranteeing the security and confidentiality of the personal data processed by AFIU, has examined the legal basis (i.e., the AML Law), which governs the activity of the latter and which sets out the rules for the administration of the data bases retained by this authority.

In this view, the IDP Commissioner considers that, although the important elements related to the security of personal data, levels of access and traceability of the processing actions are *ipso jure* reflected in the obligations that AFIU has as a public controller[211], it is necessary that further measures be taken for addressing other indispensable elements of the personal data protection legislation, which should better reflect the rights of data subjects, the obligations of AFIU as a controller, the principles of personal data protection (especially with regard to the data retention period[212]), as well as the measures guaranteeing the security of the information security management system as per Instruction no. 47 of the IDP Commissioner.

The IDP Commissioner observes that AFIU has in place, *inter alia*, procedures and rules related to the security and confidentiality of the information, but these measures are incomplete, as there is a lack of a strategy for the implementation of the information security management system (i.e., as required under Instruction no. 47).

b. *Findings regarding NBC[213]*

According to the report of the IDP Commissioner, NBC has in place specific regulations on personal data processing and protection. Such regulation includes, *inter alia*, the processing activities of NBC, the principles and criteria of personal data processing, as well as provisions on the security of the processing activities.

However, IDP Commissioner notes that there is a lack of periodic monitoring strategy

209 Report of IDP Commissioner in the ambit of the Parliamentary Resolution, dated 28.12.2020.

210 Report of IDP Commissioner in the ambit of the Parliamentary Resolution, dated 28.12.2020, page 19.

211 Here are meant the provision of article 22(gj) of the AML Law, where it is – generally – stated that the processing of personal data is carried out in accordance with the rules of the applicable legislation on personal data protection.

212 As mentioned in point (i) of subchapter VI.1 of this Report, article 16 of the AML Law grants to AFIU a vast discretional room for purpose of extending the retention term of the data processed by the Obliged Entities.

213 Report of IDP Commissioner in the ambit of the Parliamentary Resolution, dated 28.12.2020, page 15.

regarding the efficacity of the information security management system, which is crucial for the fulfillment of the information security and personal data protection requisites.

It is to be noted that, as at the time of the inspection visit that the IDP Commissioner has performed at NBC, the UBOs Registry was not yet established[214]. As such, the report of the IDP Commissioner does not mention any specific concerns in this regard.

c. *Findings regarding GTD[215]*

Pursuant to the report of the IDP Commissioner, GTD has in place a series of regulatory acts, which include provision on preservation of confidentiality of information.

However, it is observed that there are no specific norms dealing particularly with the processing (i.e., retention), protection and security of personal data, in the ambit of the processing activities carried out by this authority.

The report states that GTD does not carry out standardized and periodic monitoring process regarding, among the others, the protection of integrity of the personal data, as well as for purpose of accounting to the standards of availability and confidentiality of information.

It is to be noted that, as at the time of the inspection visit, the Law on Registry of Bank Accounts had not yet entered in force[216]. As such, the report of the IDP Commissioner does not mention any specific concerns in this regard.

Based on the above findings, the IDP Commissioner has drawn its own (comprehensive) conclusions, and issued the relevant recommendations, for the public authorities that were subject to the inspection visits, in the ambit of the Parliamentary Resolution, which are summarized below:

1. The public authorities should have in place concrete rules that guarantee the lawful processing (i.e., especially retention) of personal data, as well as the protection and security thereof, in accordance with the personal data protection legislation;
2. It is observed a lack of legal and technical knowledge [of the staff of public controllers] regarding the accomplishment of the pertinent obligations and responsibilities of the public controllers in virtue of the legislation on personal data protection.

   Therefore, continuous training of the relevant staff is necessary and strongly recommendable;
3. The public controllers should seek the opinion of the IDP Commissioner in case of any data protection related acts/projects that they seek to establish and implement, as per the mandatory requirements of article 31(1/a) of the Data Protection Law;
4. The relationship between data public data controllers and their contracted processors (i.e., which is done as per the provisions of the public procurement legislation) should account to the obligations and legal guarantees imposed to such a contractual relationship by article 20 of the Data Protection Law and Instruction no. 19 of the IDP Commissioner;
5. The access levels, to the data possessed by the public authorities, should be clearly defined and account to the confidentiality principle, which aims at guaranteeing that any personal data related activity (i.e., carried out through ICT systems) is duly traceable and controllable.
6. The major part of public authorities (i.e., including, AFIU, NBC and GTD) need to enhance their efforts and capacities for purpose of establishing, maintaining and administering the

[214] According to the UBO Law, the deadline for the establishment of UBOs Registry was 31.01.2021.
[215] Report of IDP Commissioner in the ambit of the Parliamentary Resolution, dated 28.12.2020, page 20.
[216] The Law on Registry of Bank Accounts has entered into force in January 2021.

relevant information security management systems, in accordance with the provisions of the data protection legislation (i.e., including, without limitation, Instruction no. 47 of the IDP Commissioner).

Thus, according to the report of IDP Commissioner, it is of substantial importance that the data protection related [internal] acts and the respective information security infrastructure is further modernized, in order to overcome the current difficulties and struggles that these controllers are experiencing or would experience in the future;

7. Continuous improvement of the human and ICT resources is crucial for having an adequate information security management system in place, for purpose of achieving and maintain the confidentiality, integrity, availability and resilience of information security.

   In this regard, the IDP Commissioner, recommends to public data controllers to achieve compliance with the standard ISO/IEC 27001 as updated.

The conclusions and recommendations of the IDP Commissioner deliver a clear picture of the institutional behavior of public controllers toward the accomplishment of their data protection related obligations and responsibilities.

(iii) Institutional approach from the perspective of interviews and Focus Group Discussion.

As already indicated under Chapter III of the Report, for purposes of assessing the institutional approach of stakeholders which are subject to AML legislation, vis-à-vis their compliance with data protection rules, interviews with 12 public and private stakeholders were conducted, whereby conclusions were drawn.

These conclusions acquire additional value in the loop of a comparative review toward the ones resulting from the inspective activity of the IDP Commissioner, in connection with AML legislation stakeholders.

With regard to interviewees, two different kind of classifications may apply to distinguish them, namely in: (a) Obliged Entities and supervisory authorities, or in (a) public and private stakeholders.

From the information collected through interviews (based on declarations of the interviewees), it seems that the public stakeholders are generally compliant with data protection rules, with few exceptions.

The approach of the interviewees was very positive in terms of readiness to respond to the request for interview and efforts to provide as much as possible information. However, when we compare the information collected by means of consultation of the Report drafted by the IDP Commissioner in virtue of the Parliament Resolution, with the outcome of interviews, a discrepancy is noticed in the findings.

For example, if we refer to the findings of the Report of the Commissioner, there are documents and/or systems which seem to be kept appropriately by a certain stakeholder, whilst during the interview the response to this question was negative.

This fact leads to the conclusion that most probably the person delivering the interview did not have any information on the inspective visit payed by the IDP Commissioner to the respective public stakeholder and, accordingly, that they were not the persons particularly engaged on

data protection issues within the organizational structure of the public stakeholder.

From the scrutiny of the interviews the following findings might be observed:

a. In most of the public stakeholders interviewed, with few exceptions (i.e., wherein the Albanian State Police is worth to be mentioned for the level of commitment towards data protection rules in all of the activities performed), a low level of awareness and commitment towards data protection rules is noticed. The stakeholders provided information on their level of compliance with data protection rules in the ambit of their AML related activity, but still the information provided remain generic and, in most cases, a confusion of the data protection concepts addressed in the interview could be noticed;

b. The stakeholders (or at least the persons designated to give the interview) often did not have a clear view of the separation of the responsibilities as far as obligations arising out in virtue of Data Protection Law are concerned. This can be identified from the delegation of responsibilities they do in address of Albanian Information Society Agency (AKSHI), which cannot vest the responsibilities that any stakeholders should bear on its own.

c. Another issue that the interviews could reveal is the communication channel adopted between stakeholders to transmit AML related information. Almost all of them use the transmission of information in hard copy. This arises further issues of information security due to the exposure of the information to a potentially increased number of persons which leads to potential breaches of the data privacy requirement and accordingly exposes the information to potential data breaches.

d. From the interviews' session we could notice that some stakeholders raised the classification of documents as an evidence of information security measure put in place by the stakeholder, without paying attention to the fact that classification should be supported by effective information security management systems and strict data privacy rules, which can be adversely affected by the transmission of information in hard copy or by lack of information security management systems in line with the sublegal acts enacted by the IDP Commissioner.

e. Another issue is compliance with the data minimization principle. From the interview with a supervising authority, which has specific tasks under the AML Law[217], we found out that no necessity and proportionality assessment is performed by the latter, at all, when requiring access to information by Obliged Entities in order to identify whether the obligations related to AML Law are properly fulfilled. This failure is most probably due to the lack of knowledge of data protection rules and low level of awareness in connection with data protection implications that such approach could have.

The set of interviews were followed by a Focus Group Discussion attended by several public stakeholders previously interviewed, supplemented by the attendance of other stakeholders, who provided their useful insights and contribution to the scope of this Report.

Almost same issues as described above were encountered during the Focus Group Discussion.

From the insights collected during both, interviews and Focus Group Discussion, we could reach to the conclusion that among the stakeholders attending the event, only the State Police seems to be aware of the responsibilities arising out in virtue of the 5$^{th}$ Directive. Indeed, they anticipated that they have started to get familiar with the 6$^{th}$ AML Directive already.

[217] See point (iii) under subchapter VI.1 of this Report.

The Albanian Association of Banks anticipated that a relevant number of proposed amendments/ addenda aiming to ease applicability of the law within the Albanian context, were submitted during the consultation process of the fifth amendment to the AML Law. It is still unclear which of these suggestions will be taken into consideration in the final draft that will be submitted to the Parliament for approval.

Other important issues that emerged during the Focus Group Discussion were connected with the lack of policies for destruction of the data upon expiry of the retention period and the retention period itself as already addressed this Report[218]. During the discussion taken place, the stakeholders declared that a necessity assessment on data retention was conducted by AFIU and other AML stakeholders, but the general impression was that, due to the lack of skilled staff in connection with data protection rules, such assessment does not properly address the data protection principles.

(iv) IDP Commissioner vs. Obliged Entities.

Same as in case of public controllers, the Obliged Entities (as private controllers) fall in the supervisory responsibility of the IDP Commissioner as well.

From the information obtained near the IDP Commissioner for purpose of this Report, it is noted that the latter has not carried out any investigation proceeding against any Obliged Entity, having as scope the compliance of the latter with Data Protection Law, whilst addressing their own obligations toward AML legislation.

Therefore, no conclusion tailored specifically for the scope of this Report could be drawn.

However, there are a couple of other – general – indicators, through which one might perceive the level of personal data protection compliance of Obliged Entities as private data controllers.

One of these indicators is the number of mandatory notifications filed with the IDP Commissioner by private controllers, as required by article 21 of Data Protection Law (hereinafter, the "**Indicator no. 1**"), as well as the number of Obliged Entities that has been registered with the registry of certified controllers held by the IDP Commissioner (hereinafter, the "**Indicator no. 2**").

Another indicator is composed of the conclusions drawn in this regard by the questionnaires carried out with Obliged Entities and the focus group discussions (hereinafter, the "**Indicator no. 3**").

*a. Indicator no. 1*:

According to the data reflected in the annual report of the IDP Commissioner addressed to the Albanian Parliament, the number of mandatory notifications as per article 21 of the Data Protection Law, until 31.12.2020, has reached 5,742[219].

This means that, until the mentioned date, there are only 5,742 public and private controllers that have [duly] notified the IDP Commissioner on their data processing activities. The notification process is carried out through a standard notification form.

On the other hand, the number of public controllers in Albania is around 400, whilst that of the private controllers around 170,000.

Pursuant to article 3 of the AML Law, the category of Obliged Entities includes, *inter alia*, all

[218] See point (i) and (ii) under subchapter VI.1 of this Report.
[219] IDP Commissioner's annual report for 2020, page 23.

entities licensed by the Bank of Albania (i.e., including, without limitation, banks, non-bank financial institutions, currency exchanges, etc.), the postal services carrying out payment services, stock exchanges, insurance companies, as well as their agents and brokers, and pension funds, lawyers, notaries, statutory auditors and certified accountants, real estate agents, any natural or legal person that carries out, *inter alia*, third parties' asset management, construction activities, transport activities, sale of vehicles, travel agencies, trusts, etc.

This means that the category of Obliged Entities includes a vast number of persons, who, together, significantly exceed the number of controllers that have filed the mandatory notification with the Commissioner. Alone the number of lawyers is twice big as that of the notifications filed with the IDP Commissioner by different data controllers.

From this, it can be deduced that a significant number of Obliged Entities has not yet accomplished the most basic (albeit mandatory) requirement of the Data Protection Law.

Indeed, save for the banks and most of non-banking institutions, who appear to prioritize the accomplishment of data protection requirements, the other Obliged Entities do not sound aware at all about their data protection obligations.

In this regard, the role of the IDP Commissioner is very crucial, for purpose of enhancing the pool of Obliged Entities that comply with the data protection legislation, *inter alia*, through intensification of its *in situ* investigations.

Nonetheless, considering the current number of human resources available to this authority (i.e., less than 10 inspectors for more than 170 thousand data controllers), there is not much to be expected in this context. Not to mention here the *ad hoc* obstacles such as the outbreak of COVID-19.

b. *Indicator no. 2*:

As mentioned in subchapter V.2 of this Report, as of currently, the Data Protection Law is fully approximated with the (repealed) Directive 95/46/EC.

However, the IDP Commissioner, in virtue of its sublegal acts (i.e., namely Instruction no. 48), has introduced into the domestic data protection legislation and, therewith, rendered available to the public and private controllers, the use of the certification mechanism, which, *inter alia*, aims at demonstrating compliance of data controllers with the privacy requirements of the Albanian data protection legislation (i.e., same as in case of privacy by design and by default, set out under article 25 of GDPR).

The certification is carried out by accredited organisms that are authorized by the IDP Commissioner, in accordance with the criteria and procedure set out under articles 7 and 8 of the Instruction no. 48.

Pursuant to 6 (i.e., in conjunction with article 5) thereof, the data controller might opt for certifying their information security management systems [for the protection of personal data] in accordance with the standard ISO/IEC 27001 as updated.

To this effect, near the IDP Commissioner is created the registry of certified controllers, which serves as a "white list" for the controllers registered therewith, and, thus, as an indicator for purpose of measuring the level of compliance of data controllers with the personal data protection principles and security requirements. As a matter of fact, the data controllers registered with the said registry do not become subject to *ex officio* investigation on the part of IDP Commissioner.

As such, the IDP Commissioner has given the data controllers the possibility to proactively show compliance with the data protection legislation, which, on the other hand, is supposed to enable the IDP Commissioner to concentrate its investigation resources to other controllers of different sectors.

From the review of the online registry of the certified controllers, it results that, so far, only eight controllers have opted for certification mechanisms, out of which five are Obliged Entities.

In conclusion, the present indicator shows that the number of Obliged Entities, who appear to consider the personal data protection requirements as one of their most important priorities, is very insignificant.

c. *Indicator no. 3*:

From the interviews conducted with private stakeholders, it emerges that only two (i.e., a second-tier bank and a broadcasting company) out of five were adequately aware of Data Protection Law related obligations and generally compliant with them.

From the declarations made during the interview session it seems that, especially, the second-tier bank was particularly careful to information security and data privacy requirements as well, to organize and ensure attendance of training activities for the relevant staff in connection with data protection rules organized by the bank itself, the Albanian Association of Banks and chambers of commerce of adherence of the bank.

From the declarations delivered during the interview session it seems that these two stakeholders were equipped with an information security management system updated on regular bases.

Same as in Indicator 1 and 2 above, this shows again that the level of compliance with data protection legislation on the part of the Obliged Entities, from both, quantitative and qualitative perspective, is very low.

(v) Obliged Entities vs. AML related authorities.

When attempting to assess the compliance of the Obliged Entities with the data protection legislation, an important element that is to be taken into consideration is the legal relationship between them and AML related authorities.

As indicated in the example given in page 18 of this Report, the Obliged Entities have been often required to address the request or requirements imposed by the AML authorities, even in excess/breach of the personal data protection legislation.

Thus, in many cases, the Obliged Entities have to deal with the dilemma of complying with the request of AML authorities, or with the data protection legislation.

In either case, the outcome of the dilemma would be the same; namely, the Obliged Entities would be either subject to administrative sanctions of AML legislation or those of the data protection legislation – being thus "spoilt for choice" of the fine that would be more convenient to them.

As a way of example, one might mention here the current development with the UBOs registry.

The deadline for registering the UBO with such registry terminates on 30.06.2021, otherwise a fine in the amount of ALL 650,000 (i.e., approx. EUR 5,300) would apply.

In several cases, the applications filed with UBOs Registry (i.e., held by NBC) are rejected, *inter alia*, due to the alleged lack of clear identification of the relevant UBO, as per the requirement of the UBO Law.

According to UBO Law, the Obliged Entities must identify and register the UBOs owning (directly or indirectly) 25% or more of the share capital of the Obliged Entity, or which control the latter through other forms (i.e., shareholder agreements, etc.). Thus, only the individuals that meet such requirements are to be registered with the UBOs Registry.

Under the pressure of meeting the abovementioned deadline, it is noted that Obliged Entities are filing with the UBOs Registry the whole list of shareholders of parent companies, irrespective of the fact whether they fall or not under the registration requirement.

On the other hand, NBC (i.e., as holder of UBOs Registry) appears to accept this kind of evidences/data, being thus openly in excess to the principles of personal data protection regarding a lawful processing.

The processing of personal data of individuals, who do not fall under the applicability of the UBO Law might be done only upon consent of the latter. Otherwise, the Obliged Entity would barely be considered as compliant with Data Protection Law.

This issue becomes more problematic, in cases of indirect UBOs residing in jurisdictions where the shareholders' registry is held by the company itself, not by a public authority (i.e., such as in USA and Switzerland).

This 'data protection incompliant' behavior of the Obliged Entities, relates to the different grounds.

At first, the administrative sanctions applicable in virtue of AML legislation are significantly higher than those of the Data Protection Law.

Secondly, the probability of a control on the part of the IDP Commissioner (i.e., considering the very limited human resources capacity of the latter) is very low.

In this regard, it is to be mentioned that for purpose of compliance with AML legislation, the Obliged Entities might be subject to investigations not only from AFIU, but also from their supervisory authorities, which according to article 24 of AML Law are entitled to carry out this kind of inspections and immediately notify their findings to AFIU. Not to mention here the powers of NBC (as holder of UBOs Registry) and GTD (as holder of Registry of Bank Accounts) to impose administrative sanctions to Obliged Entities for not complying with the deadlines and requirements of, respectively, UBO Law and Law on Registry of Bank Accounts.

Thirdly, there is a prevailing opinion, among Obliged Entities (i.e., especially financial institutions) that the reputation damage that might be caused to them in case of fines imposed by AML authorities is bigger than the one that would be caused by fines imposed by the IDP Commissioner for breach of personal data protection legislation.

Fourthly, the level of AML compliance that is sought to be achieved by the Albanian Obliged Entities, in the ambit oft business requirements imposed by foreign obliged entities (i.e., especially, those situated in EU and USA), when running business together, is, again, significantly higher comparing to the latter's expectations for data protection compliance.

# VII. RECOMMENDATIONS

In the epilogue of this Report the below recommendations would be brought to the attention of all AML stakeholders.

At first, it would be recommendable to achieve a as full as possible material alignment with the provisions of the 4th and 5th Directive, where applicable to the Albanian jurisdiction[220].

As such, from the perspective of the Albanian legislation, we do not identify any objective legal-formal obstacles that would impede a full material alignment of the AML legislation with the material provisions of both directives, as indicated in the ToC and briefly described under subchapter IV.4 of this Report.

Secondly, as regards, specifically, the personal data protection matters, the following would be recommended to be taken into account:

(i) There is the need to have the provisions of all AML legislation instruments harmonized with one another, as well as align them with those of the Albanian data protection legislation (i.e., including, without limitation, principles and criteria of processing, data retention terms, level of access, and other related data processing matters).

This would pledge for ensuring the compliance with the legal certainty principle, which would allow all AML stakeholders to predict their institutional and personal behavior vis-à-vis Data Protection Law provisions, when, simultaneously, addressing the requirements of AML legislation.

To this effect, the opinions of the IDP Commissioner (i.e., as per article 31(1/a) of Data Protection Law) emerge to be indispensable.

Another option would be the incorporation of legal provisions in the AML legislation that enables the IDP Commissioner the issuance of binding sublegal acts (i.e., instructions) tailored specifically for the AML sector. These sublegal acts might be issued alone by the latter, or in virtue of joint instruments with the relevant AML related authorities.

Moreover, general guidelines on the part of the IDP Commissioner, despite not being mandatory, would also contribute to this purpose;

(ii) The data protection awareness and the relevant human resources capacities within the AML related authorities and Obliged Entities should be increased.

In case of AML related authorities, this would contribute not only to their compliance with data protection legislation as public data controllers, but also would be a benchmark for the Obliged Entities in regard as well.

Moreover, this would eliminate the compliance dilemmas and pressures that the Obliged Entities, in practice, are often subject to, when addressing the requests of AML authorities that are in excess to the requirements of the data protection legislation.

In this view, periodical training to the staff of AML related authorities, in close cooperation with IDP Commissioner would be recommendable. Indeed, this would also enable the staff of the IDP Commissioner itself to become more familiar with and aware of the AML legal environment,

[220] As shown in the ToC, there are specific provisions which cannot be approximated due to the fact that Albania is not yet member of EU.

which would be surely reflected in their supervisory approach when investigating, especially the Obliged Entities.

Moreover, it would be recommendable that all AML stakeholders procure and ensure a closer cooperation between their AML departments and Data Protection Officer (DPO). The intertwining of the effort and capacities of these roles, within the organization of an AML stakeholder, would help the latter to achieve and maintain compliance with both legislations (i.e., AML and data protection one).[221]

The more this intertwining is functional, the more legal compliance would be achieved and, thus, the higher the compliance confidence of the AML stakeholder (i.e., in their own capacities) would be;

(iii) Clear and very well-reasoned and accurately outlined levels of access to the personal data should be granted to third parties, who are entitled thereto by letter of law[222]. The levels of access should be clearly determined, both, in relation to internal staff and third parties outside the organization, so to keep track of the processing activities and accessing persons.

Especially, with regard to the third parties, outside the organization of the relevant data controller, clear terms of personal data processing should be set out under the mandatory agreement that governs the relationship between the controller and data processor, in accordance with article 20 of the Data Protection Law and Instruction no. 19;

(iv) The AML stakeholders should increase and periodically review their technical and organizational measures aiming at ensuring and guaranteeing the confidentiality and security of personal data they process.

This relates, *inter alia*, to the secure channels of communications and data transmission/ transfer, between the AML stakeholders, for purpose of compliance with AML legislation (i.e., including, but not limited to, in case of due diligences, reporting, etc.).

To this effect, an updated information security management system (ISMS) for the protection of personal data, in accordance with the provisions of Instructions no. 47 and 48 of the IDP Commissioner, would be strongly recommendable.

The periodical audits of ISMS would be a necessary to achieve this. Moreover, were possible, the use of certification mechanism as per Instruction no. 48 would also be helpful in this regard.

[221] This appears to be especially crucial, in the ambit of the provisions of article 24 of AML Law as examined above, in point (iii) of subchapter VI.1 of the Report and as emerging from the interviews and Focus Group Discussion described under section III of subchapter VI.2 of this Report.

[222] See footnote 37 above.

www.transparency.mk
info@transparency.mk
www.facebook.com/TransparencyMK/
twitter.com/TI_Macedonia