C1-EU-NPA
CLUSTER ONE EU NEGOTIATIONS PLATFORM – ALBANIA

KOMITETI SHQIPTAR I HELSINKIT

POLICY AND POSITION PAPER

"Legal and institutional overview of personal data protection and security in the country and their compliance with the acquis"

This publication of the Albanian Helsinki Committee (AHC) was realized in the context of the project C1 – EU – NPA, "Improving Debate on Policies and Accountability to Fulfill Basic Rights, through the creation of the Cluster 1 Albania Platform of Negotiations," implemented by four Albanian organizations, the Center for the Study of Democracy and Governance, the Albanian Helsinki Committee, the Institute for Political Studies, and the Albanian Institute of Science, with financial support from the Embassy of the Kingdom of the Netherlands in Tirana.

The views expressed in this policy and position paper are of the Albanian Helsinki Committee and do not necessarily represent the views of the donor and the implementing organizations.

Document prepared by:
Att. Erida Skëndaj, *Executive Director, Albanian Helsinki Committee*
Dr. Jonida Rystemaj, *External Legal Expert, AHC*

Contributed for statistical data:
Safete Qato, *Student, Faculty of Justice*
Senada Aliu, *Student, Faculty of Justice*

Rr. Brigada e VIII-te, Pallati "Tekno Projekt" Shk. 2 Ap. 10, Tirana-Albania
PO Box no.1752 Tel: 04 2233671
Mob: 0694075732
e-mail: office@ahc.org.al
web site: www.ahc.org.al

POLICY AND POSITION PAPER

"Legal and institutional overview of personal data protection and security in the country and their compliance with the acquis"

June 2022

CONTENTS

List of abbreviations

NAIS	National Agency of Information Society
AEPC	Authority for Electronic and Postal Communications
EU	European Union
NBI	National Bureau of Investigation
GDCR	General Directory of the Civil Registry
GDSP	General Directory of State Police
GDT	General Directory of Taxes
GDPR	General Data Protection Regulation
ECtHR	European Court of Human Rights
CJEU	Court of Justice of the European Union
SCCOC	Special Court against Corruption and Organized Crime
IP	Internet Protocol
CoE	Council of Europe
EC	European Commission
ECHR	European Convention of Human Rights
CRIPDP	Commissioner for the Right to Information and Personal Data Protection
AHC	Albanian Helsinki Committee
CEC	Central Election Commission
	Convention 108 – Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data
LPDP	Law on Personal Data Protection
NPEI	National Plan for European Integration
DP	Democratic Party
SP	Socialist Party
PDO	Personal Data Officer
USA	United States of America
ISMS	Information Security Management System
CMD	Council of Ministers Decision

EXECUTIVE SUMMARY

Personal data protection is essential as a function of guaranteeing individuals' right to privacy. In the digital context, such protection is particularly important because individuals are considerably more exposed than in the physical dimension, as consumers or users, who benefit products and services. Furthermore, the use of information technology or artificial intelligence in data processing at a large scale dictates the need to improve the standards for personal data protection. Therefore, it is essential to create a safe environment for the subjects of personal data that, at the same time, encourages the circulation of such data as a basis for the economy of data.

This document initially analyzes, from a political perspective, the deficiencies of the domestic legal framework for personal data protection, in light of the obligations arising from the country's EU accession. This analysis of compliance with EU legislation is spurred also by the massive data breaches in the past year, which showed the vulnerability of the subjects of data and the large-scale processing of personal and sensitive data without the necessary security measures.

Further on, this document analyzes positions regarding administrative and criminal punishment of massive and unprecedented breaches of the personal data of Albanian as well as foreign citizens, as a result of these breachs (of databases).

1.1 Comparative policy approach of domestic legislation and obligations arising from the EU accession process

The EU has a complete and comprehensive, primary and secondary, legislation that creates the necessary basis for personal data protection, by specific sector. This legislation has been completed and interpreted by sustainable jurisprudence of the CJEU. Therefore now, also due to its characteristics and especially extra-territorial (beyond EU) implementation, the Regulation serves as a universal standard for personal data protection.

Personal data protection in our country, aside from being a constitutional right, is also regulated the special law "On Personal Data Protection." This law represents a good basis for protecting individuals from illegal personal data processing, but insufficient for facing the challenges that have been brought about by the development of information technology and large-scale the new European standard for personal data protection and therefore, the need arises for alignment, not only in terms of respect for obligations assumed in the context the continued alignment process, but also to expand and enhance further the rights of data subjects and to increase accountability for controllers. Furthermore, another reason that dictates the need for alignment has to do with the need to adapt to a global standard in the field of personal data protection, especially regarding the transfer or circulation of personal data from and to the EU, as essential activities for the realization of data economy.

Alignment necessarily requires the approval of a special instrument that is integrated into the juridical system and the Police Directive, in order to have one standard for data protection in this specific sector and to clearly establish the duties of public authorities.

The evaluation of our legislation has pointed to a shortcoming in the fact that data subjects do not have sufficient control over their data because there are no clear obligations for controllers/processors to

inform data subjects in a clear, simple language, in a concise and transparent manner about the controller, his identity or contact information, the purpose of the data processing, etc. Furthermore, the subjects of data may not use rights such as: the right to be forgotten (or deleted from search engines) or the right to personal data portability. In this context, Albanian law does not adequately guarantee the rights of personal data subjects, from a material and procedural aspect, as will be summarized further.

On the other hand, the Law "On Personal Data Protection" puts a heavy burden on the Commissioner, assigning him the task of controlling the compatibility of the activity of controllers/processors with the requirements of the law. In practice, this competence is impossible to fulfill due to the large number of controllers/processors in the public and private sectors as well as considerable deficiencies in human and technical resources in the office of the Commissioner.

With regard to the standing of the controllers, it has been found that the legal framework in forces does not envisage a full and clear spectrum of responsibilities such as the obligation to document all personal data processing processes, the obligation to declare the breach of personal data, both to the Commissioner and to the subjects in case the latter may be harmed from this breach, the obligation to draft privacy policies, etc.

Furthermore, at the same time, it is noticed that there is no obligation that the controller include in the technical drafting of services the protection of data through privacy by design and privacy by default, in order to ensure the best protection for the subjects of personal data.

The reflection of these changes to our legal framework would lead to considerable improvement of the rights of subjects and increase the responsibilities and obligations for controllers/processors. These changes would increase the vigilance of controllers to the processes for personal data processing. That way, the law would have a positive impact on changing the culture and behavior of personal data protection actors.

The protection of personal data is not an absolute right, especially as a function of freedom expression or on issues of public interest. Therefore, article 11 of the law tasks the Commissioner to issue instructions that establish the conditions and criteria for avoiding norms of the law on special activities (such as journalistic or academic). However, this provision is not in line with constitutional provisions, which impose a certain test for limiting these rights. Referring to considerable practice of the European Courts (ECtHR and CJEU), the limitation should abide by constitutional (and convention) standards. Therefore, there is a need for the attention of the lawmaker to balance these rights with a law and in accordance with consolidated tests deriving from domestic and foreign jurisprudence.

Aside from the substantial act, problems have also been noticed in the procedural aspect regarding the implementation of the law. Reviews have found deficiencies with regard to the competences of the Commissioner and effective means of subjects for the protection of their personal data. the law does not envisage the obligation of the Commissioner to raise the awareness of controllers and subjects about the importance of personal data and especially their protection. This obligation, together with a clear and complete framework of respective rights and obligations, would serve as a basis for creating a culture of personal data protection.

The law also does not envisage other sanctions than fines that might have a deterring or advisory effect, such as counseling, warning, scolding, or reprimand, which would be applied depending on the type and gravity of the violation.

Based on the conducted analysis, it results that there is also a lack of clarity in the formulation of provisions regarding the possibility for complaint by subjects of personal data. It is not clear for the subject of personal data what the procedural ways are that they may pursue, should personal data be processed in

an illegal manner. Should the subject address the Commissioner or violator before addressing the court, or should the subject make use of these means in parallel and independently from one another? The law should clarify which are the procedural instruments are that the harmed subject might exploit.

With regard to the creation of efficacious mechanisms for the implementation of the law, we consider that one factor that has effective impact is the regime of administrative sanctions. The regime of fines envisaged by the current law does not appear to be effective. In this context, there is a need to implement a harsher regime that might also increase (albeit through "punishment") awareness about the importance of personal data protection. Administrative punishments should be proportionate to the gravity of the violations and such that they discourage future illegal behavior in the field of personal data.

1.2 Positions on punishability, responsibility and accountability, with a focus on the administrative and criminal investigation of massive breaches of citizens' data during 2021

The publication of three databases in the excel format, containing massive personal and sensitive data of a total of 2,070,000 individuals in the country,[1] with elements that make it possible to identify them, their political affiliation, vote preferences that should be secret, salary data, place of work, vehicles owned, etc., shook the entire public opinion within a very short period of time during 2021.

News of the existence of the first database, the so-called database of "canvassers" or of "voters" was initially made public in the news portal "Lapsi.al" on April 11 of last year, during the pre-election period for the country's parliamentary elections.[2] The database contained personal and sensitive data of about 910,000 voters; according to the media, it was administered by the electoral subject "Socialist Party."

On December 22, 2021, another massive data breach was extensively reported in the media,[3] about the existence of a database of about 630,000 employees in the public and private sector. The two databases, so-called of the salaries, administered in "excel" format, contained data about the name and family name, identification number and identification cards, employer (place of work) and salaries they received for January and April 2021.[4]

Two days after the massive information breach on salaries, namely on December 24, 2021, news appeared about the existence of another database, containing data of owners of vehicles for more than 530,000 citizens.[5] The database contained data such as the brand, model of vehicle, license plate, owner, and the identification card number. The list processed on "Excel" was divided into two categories, vehicles and license plates for 530,452 citizens and vehicles of companies, namely 61,513 such. The second category contained also the license plates of relevant embassies, international institutions, and organizations in the country.

Although more than 14 months have passed, the public does not know how it was possible to obtain, process, administer, and distribute these data, without their prior approval or authorization. It is disturbing that an indefinite number of people have had and may continue to have access to them due to their

1 This piece of data reflects the total of the number of individuals who appeared in the three databases published during 2021. It dose not indicate that these individuals are different as AHC cannot possess and therefore not compare the matching of data in order to reach this conclusion or not.

2 Ekskluzive/ Si na monitoron Rilindja nr e telefonit, nr ID, vendet e punës, të dhënat konfidenciale për 910 mijë votues të Tiranës – Lapsi.al

3 https://lapsi.al/2021/12/22/superskandali-dalin-sheshit-emer-per-emer-rrogat-e-mbi-600-mije-shqiptareve/

4 https://news-31.com/neës/thellohet-sandali-publikohet-databaza-me-targat-e-makinave-i22293

5 https://news-31.com/news/thellohet-sandali-publikohet-databaza-me-targat-e-makinave-i22293

dissemination through the "WhatsApp" application.

Aside from the reaction of media or non-profit organizations in the country, concerns about the massive dissemination of personal data were also reported by the European Commission,[6] the U.S. Department of State (in the annual report on the state of human rights in the country),[7] the Limited ODIHR Mission[8] for monitoring the parliamentary elections of April 25, 2021, as well as the international organization Amnesty International[9] or Freedom House[10].

AHC notes that the lack of responsibility and impunity when actions or inaction represent a criminal offense and openly infringe upon public interest and human rights has an impact on reducing citizens' trust in the rule of law, and therefore in public institutions, thus weakening democracy. although competent bodies began administrative and criminal investigations into those responsible for these massive data breaches, to date, nobody has been punished administratively or criminally.

1.2.1 Administrative Investigation

As regards the database of voters, the Commissioner on the Right to Information and Personal Data Protection noticed its massive and illegal dissemination, through two internet websites,[11] on which on 16.04.2021 and 19.04.2021, it addressed the AEPC and the General Directory of State Police to block them immediately and start legal proceedings on the persons possessing these pages. Based on documentation made available to AHC, it is unclear when these pages were created, when they were blocked, and whether there was collaboration in the context of administrative or criminal proceedings between these responsible institutions (AEPC, GDSP and CRIPDP) on obtaining and exchanging information in the interest of the efficacy of investigations.

Although news in online media about the existence of the voters' database dates back to April 11, the order for an administrative investigation by the CRIPDP on responsible institutions that had access to some of these data began 8 days later, namely on 19 April 2021. AHC notes that this investigation began in an inverse manner from a chronological standpoint, harming the efficacy of the investigation in a timely and comprehensive manner. The CRIPDP ordered the start of administrative investigations into the media outlet "Lapsi.al," while the sources of information of the media should be protected in order to protect media freedom and its major mission in a democratic society. The priority for the administrative investigation was the inspection on electoral subject "SP" and responsible institutions that had access to the database that were partially part of the voters' database.

It is worth emphasizing that protection of the journalistic source applies to every administrative or judicial procedure (whether civil, criminal, or administrative) and in any case, it may be the last resort for searching evidence if it fulfills the test of proportionality and is in keeping with limitations envisaged in article 10, paragraph 2 of the ECHR.

It is worth noting that the electoral subject "SP," on which the suspicions made public in the media rest, has been listed by CRIPDPD last in the list of subjects under administrative investigation, while

6 file:///C:/Users/user/Downloads/Albania-Report-2021%20(6).pdf p. 28-29
7 ALBANIA 2021 HUMAN RIGHTS REPORT (state.gov) p.10
8 https://www.osce.org/files/f/documents/4/c/495052.pdf p. 19
9 Everything you need to know about human rights in Albania - Amnesty International Amnesty International p.68
10 https://freedomhouse.org/country/albania/freedom-world/2022
11 www.patronazhisti.com and https://adfrehasdgfh.web.app/

representatives of the subject declared publicly that they have a database that they have built for years of organization, contacting voters door to door.[12]

The Office of the Commissioner states that it received 81 complaints during the period April – August 2021, which have to do with the verification of the lawfulness of the processing of personal data of citizens/voters. Half of these complaints were submitted against the electoral subject "Socialist Party" and an overwhelming majority, but less than half, are attributed to the NAIS. This represents an indicator of the complaining individuals' perception on the responsibilities for this database.

With regard to the illegal dissemination of the category of personal data for "employees/officials" in the public and private sectors and the illegal spread of the category of personal data on "vehicle owners," the Office of the Commissioner received 47 complaints, of which 22 against NAIS and 25 against the GDT. Unlike the delayed start of investigations on the database of the canvassers, the administrative proceedings on the database of salaries began immediately after the publication.

On the database of salaries and vehicles, the Office of the Commissioner did not order an administrative investigation into the media subjects that made the story public.

The orders of the Office of the Commissioner on the administrative investigation into the three databases, in our opinion, are not complete, as they lack guidance on procedural actions and the tools to be used by inspectors for searching evidence, as well as how far concrete investigations into each controller should go. The concretization and individualization of the administrative activity would be essential as it needed to consider whether a fact or circumstance is necessary for resolving the case, which is determined from the start of the administrative investigation (article 77, paragraph 2 of the Code).

The publication of the report on the administrative investigation on the database of voters represents a very positive step toward transparency by the CRIPDP while the contents of the report show some deficiencies with regard to the concept of an administrative investigation that should be complete, comprehensive, and effective.

The administrative investigation into the database of voters on the electoral subject "SP" and public institutions inspected appears to have been conducted partially and in a shallow manner. In our opinion, the Office of the Commissioner possessed the legal means it did not use, not seeking diverse evidence that would enable resolving the case and the concrete identification of responsibility among controllers. The information made available to AHC does not enable an overview of concrete verifications by the Office of the Commissioner at each inspected subject, what directories and ministries were subjected to inspections, what functionaries, officials or employees were questioned, what servers were inspected, broader access to computer networks, etc.

During the administrative investigation conducted at the subjects, the Commissioner submitted a list of questions and requests regarding the processing activity for personal data by the controller in question. Except for the GDCR, it is notable that the three other controllers (NAIS, SP and GDP) demonstrated a low level of collaboration in providing information and accepting responsibilities. Furthermore, AHC notes that this information has not been subjected to verification by other means of evidence searching during the administrative investigation, thus indicating in the relevant report that CRIPDP inspectors did not have access to the servers and computer systems of the inspected subjects. The lack of access is

12 https://lapsi.al/2021/04/11/alibia-e-taulant-balles-per-pergjimin-qe-ps-u-ben-te-dhenave-personale-te- qytetareve/
https://lapsi.al/2021/04/13/rama-pranon-patronazhistet-kemi-vite-qe-i-kemi-shperndare-ne-terren/

also accepted by the CRIPDP, in its official letter to the AHC that makes available the information, with the explanation that the prosecution office has imposed a sequestration measure on them. However, in concrete terms, the administrative report as well as the correspondence with AHC does not contain further information on the coordination of work without obstacles for each institution (CRIPDP and the Prosecution Office). It is unclear whether the sequestration by the prosecution office had a finite validity (as servers are essential in the work of institutions), and whether the CRIPDP could realize verifications in those equipment or systems that were not under sequestration. Another way to avoid this obstacle was to temporarily suspend the administrative proceedings until the cause creating the obstacle would cease according to provisions of the Administrative Procedure Code.[13]

The Office of the Commissioner displays a double-standard approach regarding administrative sanctions by fines on the subjects that did not collaborate fully during the administrative investigation on the voters' database. Due to lack of collaboration, CRIPDP issued a delayed sanction only on the GDT, four months after the administrative investigation began. Meanwhile, no such sanctions were applied on the NAIS and electoral subject SP, although part of the information was absent from these two subjects, during the administrative proceedings. In the fact of the fact of limited collaboration and the approach of public officials of the inspected subjects to avoid responsibility, assigning such responsibility to one another, the CRIPDP could have escalated legal tools with a criminal referral to the prosecution office for elements of abuse of office (article 248 of the Criminal Code[14]).

It is also notable that part of the responses that avoid providing information from the GDT have been formulated in the same way as the NAIS responses, thus raising reasonable suspicions about the exchange of information between these two institutions during the administrative investigation conducted by the CRIPDP.

In spite of the obligation to create, administer, and maintain the Information Security Management System (ISMS), the CRIPDP has found that the ISMS has been absent from almost all public bodies that have been investigated administratively, including the electoral subject SP. For public authorities that have been inspected before the news was published about the voters' database, these deficiencies have been reflected in annual reports of the CRIPDP to the Assembly. Nevertheless, this alert by the CRIPDP did not help prevent the incident while the reiteration of the lack of this system during the administrative investigation on the voters' database did not serve as a necessary cause for administrative punishment.

It is also notable during the administrative investigation that the GDP and the SP made available partially the requested information in a delayed manner, namely 20 and 40 days from the day when the administrative proceedings began. This delay creates potential premises for the alteration or hiding of necessary evidence, for which the Office of the Commissioner did not request, in keeping with the Administrative Procedure Code, to secure them at the start of the administrative investigation (such as

13 According to article 23 of the Administrative Procedure Code, if the final decision on an administrative proceeding depends on making a preliminary decision, which is within the competence of another administrative body or the court, the body that has the competence to make the final decision suspends the relevant proceeding until the other administrative body or the court have made that prelieminary decision. Exemption from this rule is only allowed in those cases when failure to make an immediate decision causes irreparable damage to the fundamental constitutional rights of the parties.

14 The intentional commission or non-commission of actions or inaction in violation of the law, which represents a failure to fulfill duties, by the person exercising public functions, when it has brought him or other persons unjust material or nonmaterial benefits and have harmed the legitimate interests of the state, of citizens, and other legal persons, if it does not represent another criminal offense, is punishable by imprisonment of up to seven years.

the servers or other sources of evidence might have been).

At the end of the administrative investigation into the three subjects (public controllers), the CRIPDP reaches hypothetical conclusions that the possibility may not be ruled out that data for the database of the canvassers were taken from the database controller and/or processed by these institutions or subjects contracted/subcontracted by them. These conclusions do not serve at all public interest and weaken the responsibility and accountability of the subjects that were administratively investigated.

The CRIPDP conclusion on the "SP" electoral subject that the database of about 910,000 voters may have been created by certain party and organizational structures at the local level, by candidates, or subjects contracted or subcontracted by them, in violation of the internal regulations of organization of this controller, is not convincing in the eyes of public opinion and bears elements of subjective bias, minimizing the responsibility of the subject itself as a single political organization.

It is unclear why in the circumstances of disrespect for legal provisions that have to do with maintaining and processing personal data, the CRIPDP did not issue an administrative punishment by a fine for any of the inspected subjects, according to article 39 of law no. 9887/2008.[15] At the end of the investigation, the CRIPDP reached only general recommendations for the subjects, which do not envisage deadlines within which they should be fulfilled. These recommendations would be appropriate in the context of a thematic inspection and not in a case of high public sensitivity, where the priority was on identifying responsibilities for the breach, unauthorized processing and administration of personal and sensitive data in the database of 910,000 voters.

1.2.2 The Criminal Investigation

Immediately after the publication in the media of the story about the existence of the voters' database, the Special Prosecution Office began a criminal investigation upon its own initiative, merging the case with the criminal referral filed by the electoral subject "DP" for the criminal offense of "active corruption in elections." Upon registration of the proceedings, SPAK immediately asked for the sequestration of computers and working equipment of the media portal "Lapsi.al," which was the first to publish the news of its existence. The SPAK request was accepted by the first instance SCCOC by decision no. 131, dated April 18, 2021.[16] Three days later, on April 21, the ECtHR ordered the Albanian state to stop the execution of the sequestration decision on any equipment for the preservation of data and computer or electronic data, ruling in favor of the portal leaders with an intermediate measure, according to rule 39 of the ECtHR Regulations.[17]

Five months after the start of investigations, the Special Prosecution Office has dropped the criminal case for lack of competence, transferring it to the ordinary jurisdiction Prosecution Office (at the Tirana First Instance Court). It is noted with concern that for the database of the voters, there is no individual taken as a defendant although it has been more than one year since the initial registration of the criminal

15 Although the violations are not directly linked with the target of the administrative investigation, they still have been found and analyzed extensively in the report of the administrative report on these subjects.

16 Based on rule 39 of the Court of Justice of the European Union Regultions, the latter may impose temporary measures that are binding for the interested state. Temporary measures are applied only in exclusive instances. The court may issue temporary measures against a member state only after it has reviewed relevant information and the petitioner faces a serious risk or irreversible damage if those measures are not applied.

17 COURT-7003525-v2-20204_21_LE2_2a_R39_Granted_Only.pdf (reporter.al)

proceedings by the Special Prosecution Office.

As regards the salary database, the Tirana Judicial District Prosecution Office, has started on its initiative the criminal proceedings, immediately upon publication of the story. On this, there has been no criminal referral. During the investigations, the criminal offense has been attributed to two specialists of NAIS and 2 private sector employees. In a press conference held by the former Chief Prosecutor of the Prosecution Office at the district court and the State Police on January 7, 2022, it appears that the investigations on the publication of salaries and license plates were conducted simultaneously as the same perpetrators have been accused for both cases.[18] Meanwhile, the announcement by this prosecution office on the conclusion of investigations regarding the publication of salaries 4 months later, there is no information regarding the case of the license plates or vehicles. Furthermore, in reference to information made available partially to us by this prosecution office, we notice that the data refer to criminal investigations on the salary database and not the vehicles' database.

In the context of investigations by the Tirana Judicial District Prosecution Office on the salary database, the hard disc that was inspected and belonged to one of the defendants also contained a considerable number of other documents with bank data on various clients. This element is disturbing in terms of security of other data. it is unclear how such data were obtained and whether the prosecution office made any referrals for administrative investigation of subjects (controllers in the banking sector or beyond) that are in contact with such data.

The investigation by the prosecution office, aside from needing to be complete, objective, and comprehensive, should also be efficacious and be carried out in a reasonable time. Otherwise, there is a risk that evidence may be damaged, manipulated, or even eliminated. The length of the criminal investigation with regard to the personal data of employees' salaries appears to have been 5 months. the Tirana judicial district prosecution office carried out the investigation within a reasonable time period given the complexity of the case.

Based on the official announcement on the conclusion of criminal investigations into the salary database, it appears that the Tirana judicial district prosecution office carried out the investigations on 2 employees of NAIS on the charges of "Abuse of office," "Passive corruption of persons carrying out public functions," and for the other 2 defendants, employees in the private sector, for the criminal offense of "Active corruption of persons carrying out public functions." Referring to article 75/a, letter "a" and article 80, paragraph 1 of the Criminal Procedure Code, it is notable that two of these offenses (article 244 and 259 of the Criminal Code) are the material competence of the Special Court against Corruption and Organized Crime. It is unclear under what conditions and circumstances and, therefore, on what legal basis these citizens were investigated by the Tirana Judicial District Prosecution Office for criminal offenses that are within the material competence of SPAK and the SCCOC.

AHC requested from the Special Prosecution Office copies of decision making on the start of criminal proceedings and the dropping of the proceedings on the voters' database as well as further pursuit of the cases by the prosecution office of the Tirana judicial district. This information was not made available to AHC. The Special Prosecution Office avoided providing a response, referring us for more information to the Prosecution Office of the Tirana First Instance Court. The focus of AHC's request for information was whether SPAK investigated high-level functionaries of the institutions that such data is suspected to have

18 https://a2news.com/2022/01/07/skandali-i-publikimit-te-pagave-4-te-arrestuar-prokuroria-zbardh-skemen-do-ti-shkohet-deri-ne-fund-cdolloj-subjekti-te-perfshire/

been breached from (NAIS, Ministry of Economy and Finance), collaboration between the prosecution offices and other law enforcement and public bodies pertaining to the investigations, whether there were difficulties in obtaining and collecting evidence, etc. Such information of high public interest, although the criminal case has been dropped by the Special Prosecution Office because of lack of competence, has not been made public yet.

Based on the provision of the law on the right to information no. 119/2014, AHC filed a complaint with the office of the CRIPDP, which addressed the two prosecution offices with a request to provide information. Still, the prosecution offices avoided making full information available to the AHC. Although the country is in an important phase of reforming the justice system, we notice a still closed approach of the prosecution office for making available information requested by AHC, which would enable an objective and more comprehensive analysis of the progress and effectiveness of investigations, deadlines of the investigation, collaboration between institutions, decision making by the prosecution office, etc.

INTRODUCTION

The economy and society in general have undergone considerable changes due to the development of information technology. At the center of such changes are data (not just personal ones), because most part of the economy functions on the basis of data, innovation and science are based on data for further advancement.[19] The appropriate processing and use of data helps encourage market competitiveness, the improvement of health, the environment, and governance in general.[20] Therefore, it is necessary that data serve these goals without infringing upon the privacy of the subjects of data. In other words, in a digital economy and society, data is the raw material to increase benefits for individuals, but these processes should adhere to legal limitations. That is why norms have been established for the protection of personal data that seek to outline the limits of their processing. In general, such norms have a double purpose; at the same time, they protect personal data of individuals as well as allow the circulation of data, according to established terms.

In our country too, personal data protection, aside from the prescription at the constitutional level, has also special legal regulations that establishes the conditions and limits of the processing of data by public authorities and private entities. The law in force has been drafted by taking as a model Directive 95/46/EC on the protection of individuals' data regarding the processing of personal data and their free circulation. Nevertheless, the European Union undertook a comprehensive reform in the field of personal data protection that was finalized in 2016 with the approval of a package with this focus, where we single out the General Regulations for Personal Data Protection. These regulations serve as the basic framework for personal data protection that has strengthened the rights of subjects, has increased transparency, has increased the responsibility of subjects administering data, and has re-dimensioned the role of oversight authorities.

Based on this reform in the European Union and on the continued requests of the Commission to harmonize domestic legislation with the acquis, this policy document seeks to highlight the level of compliance of our law "On Personal data protection." Furthermore, the document also seeks to point to the weak points of the law that had an impact on the massive data breaches and how the new European standard helps prevent such phenomena in the future. At the end of the analysis, considering the behavior of domestic authorities to the three massive data breaches (some of a sensitive character), the document provides some valuable recommendations for improving the law in force.

1.1. Context

The European Commission Report on Albania for 2021 states that efforts continue to align personal data protection with the General Regulation for Data Protection 2016/679 and the Police Directive 2016/680. Albania has approved in principle the Protocol for the amendment of the Convention on Protection of Individuals regarding the automatic processing of personal data, thus opening the way to its signing. In general, the European Commission recommends to Albania to update the security system, limiting access

19 European Strategy on Data, 19.2.2020, accessible at (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN)

20 European Strategy on Data, 19.2.2020, accessible at (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

to and the use of databases administered by the state where personal data are kept.

For almost a decade and a half, namely on March 10, 2008, Albania approved law no. 9887 "On Personal Data Protection," which underwent amendments twice, namely in 2012 and 2014, by law no. 48/2012 and law no.120/2014. The object of this law is to establish the rules for the protection and legal processing of personal data, which is realized by respecting and guaranteeing fundamental human rights and freedoms and, in particular, the right to preserving a private life.[21] According to this law, the CRIPDP is the responsible independent authority that oversees and monitors protection of personal data, in accordance with the law. The CRIPDP enjoys among others the competence to conduct administrative investigations and have access to the processing of personal data, as well as collect all necessary information for fulfilling its oversight duties; the competence to order the blocking, deletion, destruction, or suspension of the illegal processing of personal data. In cases of serious, repeated, or intentional violations, the CRIPDP sanctions administrative violations, may issue punishment of a fine, file a referral with the prosecution office, and publicly denounce or report the case to the Assembly and the Council of Ministers.

The protection that the state offers to individuals regarding privacy is not only in the context of the public right, but also enjoys special protection in criminal legislation. Article 121 of the Criminal Code sanctions as a criminal offense the unjust interference in private life, which among others is also realized with preservation for publication or publication of data that expose an aspect of the person's private life without the person's consent. This criminal offense is punishable by a fine or imprisonment up to two years. Based on how the criminal offense is committed, we may be in front of the fact that the offense really compete with other criminal offenses that are sanctioned in the Criminal Code, such as Abuse of Office (article 248 of the C. Code), Active corruption persons who exercise public functions (article 244 of the C. Code), Active corruption of high state functionaries who exercise public functions or locally elected persons (Article 245), Passive corruption of persons exercising public functions (article 259), Passive corruption of high state functionaries or locally elected persons (article 260), Interference with computer systems (article 293/c), etc. In such cases, the position of the accused persons is aggravated and their conduct is punishable by two norms at the same time, thus leading to a harshening of the punishment given that we have to do with the violation of a norm that represents a criminal offense.[22]

If violations of the provisions of legislation that protect personal data represent administrative and/or criminal violations, our legal framework envisages the necessary and adequate procedural guarantees that the administrative investigation conducted by the CRIPDP and the criminal investigation by the prosecution office is complete, comprehensive, objective, and effective. Respect for the deadlines of administrative procedures and criminal investigations are requirements envisaged expressly in our Administrative Procedure Code and the Criminal Procedure Code.

The massive breaches of personal and sensitive data during 2021 highlighted the urgent need for protecting citizens from the violation of their data and the necessity for accountability, responsibility, and transparency, on the perpetrators of these databases but also of the institutions that the law tasks with the duty to resolve and punish perpetrators. The publication of the news about these databases drew also the attention of international actors who highlighted concern about the security of such data. Namely:

- The European Commission Report on Albania for 2021 underscored that the CRIPDP started on its own initiative an administrative investigation on the breaches of sensitive personal data, including

21 https://www.idp.al/wp-content/uploads/2020/03/Ligj_Nr.9887_dat%C3%AB_10.3.2008_i_ndryshuar.pdf
22 Unifying Decision of the United Colleges of the High Court, no. 3, dated 02.11.2015

political preferences in the context of the campaign for the April 25 parliamentary elections. The CRIPDP issued recommendations to relevant authorities about updating the security protocols and limiting access and the use of personal data maintained in state databases. The institution has issued a decision to impose sanctions against tax authorities for lack of cooperation. The European Commission asks for the fast pursuit of these recommendations, without prejudice toward other procedures by competent authorities that aim at evaluating the integrity of the electoral process.

- The final report on the April 25, 2021, parliamentary elections by the ODIHR Limited Election Observation Mission highlights that the unauthorized sharing or combination of voters' personal data for the supposed purposes of democratic engagement may be considered a violation of the commitment to protect the right to privacy and family life. This may harm the trust of the electorate, including trust in the secrecy of their vote.[23]
- According to the 2022 report of Freedom House on Freedom in the World, in Albania, critics, including members of the opposition, accused the Socialist Party of stealing data from official government sites and used them to 'intimidate' voters. The Socialist Party denied continuously that the database was created or used illegally.

1.2. Purpose of the document

The document analyzes in a strategic manner the legal and institutional framework in the country on personal data protection, seeking to identify shortcomings, non-compliance, or priority gaps that need to be aligned with EU legislation.

In order for this assessment to go beyond the theoretical aspect and is intertwined with practical aspects, a part of the document presents and analyzes the positions regarding the punishment of massive and unprecedented data breaches of personal data of Albanian as well as foreign citizens in April and December of the previous year (2021). Namely, the document analyzes the activity of the CRIPDP and the prosecution office with regard to conducted investigations (according to the material competence of the general jurisdiction prosecution offices and SPAK) on these cases.

1.3. Methodology

The first two chapters of the document, with a political approach, have in the focus of the analysis the non-compliance of the Albanian law "On Personal Data Protection" with the General Data Protection Regulation (GDPR). We underscore that this analysis does not take into consideration the law "On Personal Data Protection," which at the time of writing of this document was under review process at the Ministry of Justice. In evaluating the European legal framework in the field of personal data protection, we used different acts, directives, evaluation reports, and scientific articles and jurisprudence of the European Courts (ECtHR and CJEU). Since a long resource list was used, the analysis and evaluation of this framework is more complete compared to that of the domestic law. On the other hand, in the national context, the analysis focused on the contents of the law and the by-laws in force as well as interviews with representatives of the CRIPDP and the Ministry of Justice, given that we found a considerable lack of scientific research and jurisprudence in this field.

23 https://www.osce.org/files/f/documents/4/c/495052.pdf p. 19

This document pursues the following structure: the first chapter provides a general overview of European regulation in the field of personal data protection. Part of the treatment is also the Council of Europe's regulatory framework, given that the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data is the only international act with binding powers for the protection of personal data beyond the EU territory. The following chapter addresses the compliance of the law with the General Regulation on Personal Data Protection. This chapter addresses some of the main aspects of the law such as the rights of subjects of personal data, the obligations of controllers, and mechanisms for effective implementation of the law.

In the third chapter, the document analyzes and presents positions in quantitative and qualitative terms, on the efficacy of responsible bodies with regard to the punishment of the three precedents of massive breaches of personal and sensitive data, namely April and December 2021.

For the purposes of this analysis, the Albanian Helsinki Committee (AHC) has sought information through official requests to the CRIPDP,[24] the Special Prosecution Office against Organized Crime and the Tirana Judicial District Prosecution Office.[25]

The information requested from the relevant prosecution offices has to do with the number of criminal referrals and the subjects that set these prosecution offices into motion as well as proceedings upon the initiative of the prosecution office (ex-officio or by the initiative of the prosecution office), decision making to start proceedings, the progress of further pursuit of the cases, and the specification of the categories of perpetrators, the criminal offenses they are accused of, and the timespan of investigations. A special focus of the request for information was whether SPAK investigated high level functionaries of institutions, from which it is suspected these data breached from (NAIS, Ministry of Economy and Finance), whether charges were brought to the competent court, as well as the progress of adjudication of these cases, collaboration between the prosecution offices and other law enforcement and public bodies for the purpose of the investigations, whether there were difficulties in obtaining and collecting evidence, as well as cases of complaints against prosecution office decisions.

In official responses, the information made available by the prosecution offices was partial. They provide general information about the investigations with regard to those by initiative or those based on referrals by other subjects, the target of the referrals and criminal offenses committed, without explanations on the process and conduct of investigations by them. With regard to this part, the Special Prosecution against Corruption and Organized Crime referred us to the Tirana First Instance Court prosecution office. The Tirana First Instance Court prosecution office said in its response that it could not provide detailed information on the progress of the investigation process given the phase the investigations were at.

In the situation where information made available by the prosecution offices was partial and not complete, AHC sent two complaints to the CRIPDP on "Complaint against refusal to provide information and copies of official documents," against the Public Authority/ Prosecution Office at the Tirana First Instance

24 Request for information no. Prot 279 was sent to the CRIPDP on April 12, 2022, for making available information and documentation presented in the items of the request.
Letter of response from CRIPDP on April 22, 2022, no. prot. 793/1.

25 Request no. prot. 277, April 11, 2022, on 'request for information and making available anonymized documentation' to the Special Prosecution Office against Corruption and Organized Crime and the Tirana Judicial District Court.
Letter no. 5471/1 Prot/ S.M dated 14.04.2022 Response letter, Prosecution Office at the Tirana First Instance Court. Letter no. 2990/1 Prot dated 15.04.2022 Letter of response from the Special Prosecution Office against Corruption and Organized Crime.

Court and the Special Prosecution Office against Corruption and Organized Crime.[26]

Following the intervention of the Commissioner, the responses of the prosecution offices again lacked information on the conduct of investigations, providing the same information as in the first request. Meanwhile, on 09.05.2022, media published a decision of the Tirana First Instance Court prosecution office about the conclusion of investigations on the publication of the databases of the salaries of citizens employed in private and state institutions.[27]

The monitoring of the CRIPDP activity was realized not only to secure necessary transparency and information of the public for such matters of high public interest, but also to identify shortcomings and other needs that have to do with the capacities and the need to improve policies, in the context of obligations and requirements dictated in the context of the country's integration into the European family. Special focus in the analysis of the efficacy of administrative investigations by the CRIPDP on the voters' database, otherwise known as the canvassers' database, was the report of the Commissioner's office on the administrative investigation conducted on some subjects. In this regard, the third part devotes special attention to the adequacy of the administrative investigation regarding the tools for seeking evidence, deadlines, and other elements of the administrative procedure.

In the fourth part, the document conveys some valuable recommendations for improving the standard of personal data protection in legislation and its full alignment with the GDPR, as well as institutions responsible for the protection of personal data when they are violated in contravention of the law and, therefore, sanctioned administratively and/or criminally.

26 Complaint no. 908 Prot dated 04.05.2022 on "Complaint against the refusal to provide information and copies of official documents," against the Public Authority/ Special Prosecution Office against Corruption and Organized Crime to the Commissioner for the Right to Information
Complaint no. 908/1 Prot dated 04.05.2022 on "Complaint against the refusal to provide information and copies of official documents," against the Prosecution Office of the Tirana First Instance Court
Letter no. 6708/1 Prot/ M.XH dated 11.05.2022 Letter of response from the Prosecution Office at the Tirana First Instance Court
Letter no. 2990/3 Prot dated 10.05.2022 Letter of response, Special Prosecution Office against Corruption and Organized Crime.

27 https://shqiptarja.com//uploads/ckeditor/62840c6b88a45CamScanner%2005-16-2022%2023.14%20(1)_001.pdf .

CHAPTER I

A. European Regulatory Framework in the Field of Personal Data Protection

1. General Regulation on Personal Data Protection

Personal Data Protection is a fundamental right included in the European Charter of Fundamental Rights. Article 8 of the Charter establishes that everyone has a right to protection of personal data linked with that person.[28] Indeed, the fundamental right to protection of personal data should be considered a new *Habeas Corpus, in terms of the inviolability of the person in the electronic dimension.*[29] In order to provide full and effective protection of personal data in the European Union, special legislation on personal data protection has been approved. The General Regulation for Data Protection (also known as GDPR) was approved in 2016.[30] Although approved since 2016, its effects began in 2018, which was accompanied by added attention of practitioners and theoreticians. The mentioned regulation continues, although in an improved context, the tradition of personal data protection created by Directive 95/46/EC on the protection of individuals' data regarding the processing of personal data and their free circulation. This directive served as the bed on which the GDPR was built, integrating also the practice of the Court of Justice of the European Union as well as new concepts related to technological development and virtual reality.[31] In fact, the Directive served also as a basis for the European Charter of Fundamental Rights, which recognizes autonomously the fundamental right to data protection, certainly linked with the right to privacy. Directive 95/46/EC began as an attempt to harmonize pre-existing legislations of the Member States.[32] While the approval of the regulation was dictated by the need to further align personal data protection by the Member States and to update this existing framework with new technological developments.

Below, the paper mentions briefly other acts approved in the European Union that, although they are not the main focus of this document, do bear relevance on personal data protection. The purpose for including them has to do with providing a complete framework regarding the standard of personal data protection provided by the EU.

2. Police Directive

Aside from the mentioned regulation, the EU's regulatory framework on personal data protection includes the approval of Directive 2016/680 on the protection of physical persons from data processing by competent authorities for purposes of prevention, investigation, discovery, or prosecution of criminal offenses or

28 Article 8, European Charter of Fundamental Righs https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

29 See S. Rodota, "Data Protection as fundamental Right", in S. Gutwirth et al, (Eds) Reinventing data Protection?, Springer 2009

30 Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016

31 Th. Streinz, The Evolution of European Data Law, published in P. Craig and G. de Burca (eds), The Evolution of EU Law, Oxford University Press, 2021, p. 902-936.

32 Th. Streinz, The Evolution of European Data Law, published in P. Craig dhe G. de Burca (eds), The Evolution of EU Law, Oxford University Press, 2021, f. 902-936.

execution of criminal decisions and the free circulation of these data.[33] This directive has a defined focus that only relates to personal data processing in the criminal sphere, thus creating the necessary conditions for the processing of data by public order bodies while not violating the fundamental rights of individuals. The directive was approved at the same time as the Regulation and reflects the same standards as the regulation, but adjusting it to the nature of activity of criminal field authorities. The approval of these two acts together, in one package, aims at the simultaneous presentation of standards for personal data protection in each sector.

The directive created a more inclusive framework in the field of protection of personal data that are on the same line with obligations stemming from the Regulation and include exceptions as necessary.[34]

3. Privacy Directive in electronic communications

The electronic privacy directive[35] is another important instrument that completes and often times surpasses the General Data Protection Regulation because this directive refers exclusively to the processing of personal data and protection of privacy in electronic communications. There is an organic connection between these two instruments because the basic principles of personal data protection derive from the Regulation while the directive complements with the specific requirements dictated by the special sector it covers, thus serving as lex specialis. Thus, in this way, it has a much more limited field of application. The directive applies to the sector of telecommunications due to the specifics that it reflects as well as due to developments in the information society. The directive establishes the obligation to notify and obtain the consent of internet users before the latter use tracking cookies or similar technologies.[36] In the spirit of the Regulation for Personal Data Protection, for approval for processing to be considered valid, it should be an indicator of the clear, free, specific, informed will of the subject of personal data for the processing of data related to that person.[37] Nevertheless, there are exemptions when the consent is not necessary and these have to do mainly with necessary cookies for offering services and the realization of communication.[38] Due to the update of these main acts of the EU on personal data protection, the need has arisen to update this directive. This project is ongoing and very soon the approval of the Electronic Privacy Directive,[39] which will replace the directive in question, is expected.

33 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.

34 European Data Protection Supervisor, Opinion 6/2015, A Further Step Towards Comprehensive EU Data Protection, 28 Tetor 2015, p. 4.

35 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended.

36 Article 5(3), Electronic Privacy Directive

37 See Article 4(11), GDPR

38 Ibid.

39 See proposal for Regulation: https://eur-lex.europa.eu/legal- content/EN/TXT/?uri=CELEX%3A52017PC0010, accesseed on 26.4.2022

4. Regulation 2018/1725

Due to the special form of organization, the EU has approved a special act that covers the protection of personal data of individuals from the activity of the EU's own bodies. therefore, Regulation (EU) 2018/1725[40] establishes the obligation of EU institutions on personal data protection, by updating the previous regulation[41] with the new standards included in the General Personal Data Protection Regulation.

5. Jurisprudence of the Court of Justice of the European Union

The jurisprudence of the CJEU has played a special role in advancing the concepts of Directive on personal data protection. Through its caselaw, the court has clarified, advanced, and introduced other rights of the subjects of personal data. As a matter of fact, there is a rich CJEU caselaw also on personal data protection, mainly in terms of interpretation of provisions of the mentioned directive. As per the implementation and interpretation of the provisions of the Regulation, there is a lack of practice because it is a relatively new act. Nevertheless, two of the most worthwhile cases to be mentioned include the so-called Schrems II and Google Spain.[42]

In the first case, Mr. Schrems complains about the transfer of his personal data from Facebook Ireland (headquartered in the EU) to Facebook Inc. (headquartered in the U.S.), because the state to which the data is transferred does not offer the same guarantees as Ireland. In fact, this is the second case by Mr. Schrems, raising the same concern, but now in the context of the Regulation on Personal Data Protection. In the first case,[43] the CJEU invalidated the decision of the Commission 2000/520/EC of July 26, 2000 (known as Safe Harbour) as it did not offer the same level of protection as the EU regulatory framework.

For that reason, a new EU-USA agreement was negotiated, termed Privacy Shield, after the Commission evaluated the USA legislation.

In this case, the Court considers that "…appropriate guarantees, applicable rights, and effective legal means required by these provisions should ensure that the subjects of data, whose personal data are transferred to a third country, in keeping with the standard data protection clauses, should be offered essentially the same protection as guaranteed inside the European Union by this regulation, as read in light of the charter. To that end, the evaluation of the level of protection provided in the context of such transfer should, in particular, take into consideration both contractual clauses agreed upon by the controller or processor set in the European Union and the receiver of the transfer located in the third country in question and, with regard to any access by public authorities of a third country to the transferred personal data, the relevant aspects of the legal framework of that third country, especially those established in a non-exhaustive manner in Article 45(2) of this Regulation.[44]

40 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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 (Text with EEA relevance.)

41 Rregullorja (EC) 45/2001

42 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317.

43 Maximillian Schrems v Data Protection Commissioner, C-362/14,ECLI:EU:C:2015:650

44 Pg. 105, Maximillian Schrems v Data Protection Commissioner, C-362/14,ECLI:EU:C:2015:650

The court raises the concern that the decision of the Commission, referred to as Privacy Shield "this intervention may arise both from access and use of personal data transferrable from the European Union to the United States by American public authorities…"[45]

The Court considered that "the notification/communication of personal data to third parties, for instance, public authorities, represents an interference with fundamental rights regulated by Articles 7 and 8 of the Charter, notwithstanding the continued use of communicated information."[46]

In the second case, the court preceded the Regulation as it advanced even further the right of subjects of data to erase their data. In fact, unfortunately, this right "created" by the court is "the right to be forgotten," in which the court maintained that "…the subject of data, in light of his fundamental rights according to articles 7 and 8 of the Charter, has the right to request that the information in question no longer be made available to the broader public through inclusion in a list of results and the position should be taken that, as paragraph 81 of the current decision continues, that these rights prevail, as a rule, not only over the economic interests of the search engine but also the interests of the broader public to find that information through a search about the subject of data."[47]

6. Novelties of the General Data Protection Regulation (GDPR)

The approval of the Regulation was seen in the European Union as a moment of importance toward strengthening the regime for personal data protection, especially at a time when technological developments considerably expose our personal data. In almost every obtained service, the citizen gives out continuously personal data. This exposure is even more sensitive in terms of activities carried out in the electronic dimension. Therefore, the selection of such an instrument, the Regulation, sought to avoid the fragmentation of protection for citizens of the European Union (EU). This goal was going to be fulfilled also through the same interpretation of this act by the Court of Justice of the European Union.[48] This way, a higher level of legal certainty is provided for personal data protection everywhere in the EU.

In general terms, the Regulation strengthened the rights of subjects of personal data and assigned more obligations for controllers and processors.[49] With regard to individuals' rights, the Regulation recognized new rights, thus increasing transparency and increasing the control of subjects over their own data.[50] And for the controllers, the Regulation established more responsibilities, among others, changing the regime of fines, setting the obligation to notify the subject of personal data and determining the creation of the personal data officer.

Analyzing all the positive changes that the Regulation brought about toward personal data protection, it may be concluded that this regulatory framework has almost the same place and should be evaluated just as carefully by commercial companies (which act as controllers or processors) as the norms of the right to

45 Pg. 165, Maximillian Schrems v Data Protection Commissioner, C-362/14,ECLI:EU:C:2015:650
46 P. 171, Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650
47 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317, p. 97.
48 Ch. Kuner, et al, The EU General Data Protection Regulation: A Commentary, Oxford University Press, 2021, f.9.
49 T. Mulder, Health Apps, Their Privacy Policies and the GDPR, European Journal of Law and Technology, Vol 10, no.1, 2019,
50 Communication From the Commission to the Parliament and the Council, Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the digital transition- two years of application of the General Data Protection Regulation, SWD (2020)115 final, p.1.

competition. This is due to the new enforcement mechanism and the added procedural requirements to alert deviations from the application of norms and the announcement of incidents related to data security.[51]

6.1. Meaning of Personal Data

The Regulation has a double purpose because at the same time, it seeks to encourage the free circulation of personal data inside the EU (to help businesses) and to protect personal data of European citizens.[52] Clearly, the second goal is prevalent, based on the formulation of the provision cited above. As a function of realizing these goals, the Regulation identifies two categories of personal data: personal data and a special category of personal data (known as sensitive data). 'Personal data' is considered *'any information linked with an identified or identifiable physical person; an identifiable person is the individual who may be identified directly or indirectly.'*[53] In this context, the concept of personal data is very broad, including any data that may identify an individual, besides the person's name and last name. Also, these include identifying pseudo-anonymized data, IP addresses, web page cookies, or similar data.[54] Meanwhile, the category of sensitive personal data includes data on ethnic or racial background, political views, religious or philosophical beliefs, trade union membership, data on health, data on sexual life and sexual orientation, genetical data, and biometric processing of data only for the purpose of identifying an individual. For the processing of special category data, the Regulation includes added care as it has established independently cases when their processing is allowed, as opposed to the general applicable regime for all other personal data. The Regulation is applied in cases of personal data processing, a concept that again has a very broad definition, including a series of processes, such as collection, maintenance, dissemination, deletion, archiving, etc.

6.2. Principles of legal processing of personal data

The Regulation presents a mixture of detailed and technical regulations for personal data protection. The principles on which legal processing of personal data are allowed include: the principle of lawfulness, justice, and transparency,[55] the principle of established purpose,[56] the principle of minimization of data,[57] the principle of accurate and, when necessary, updated data,[58] the principle of limited maintenance,[59] and the principle of integrity and confidentiality.[60]

51 Ch. J., Hoofnagle et al, The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, 2019, Vol 28, No.1, 65-98.
52 Article 1, GDPR
53 Article 4(1), GDPR
54 Ch. J., Hoofnagle et al, The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, 2019, Vol 28, No.1, 65-98.
55 Article 5(1)(a), GDPR
56 Article 5(1)(b), GDPR. See also article 89(1).
57 Article 5(1)(c), GDPR.
58 Article 5 (1)(d), GDPR
59 Article 5(1)(e), GDPR.
60 Article 5(1)(f), GDPR

6.3. Conditions for the legal processing of personal data

The Regulation has established six legitimate reasons for the processing of personal data: (1) the data subject has granted consent for the processing of data for one or several purposes; (2) the processing is necessary to realize a contract in which the subject is a party or to take the necessary measures before entering into the contract; (3) the processing is part of legal obligations for the controller; (4) the processing is necessary to protect the vital interests of the data subject or another individual; (5) the processing is necessary for realizing a task of public interest or the exercise of a power that has been granted to the controller; and (6) the processing is necessary for purposes of legal interests of the controller or a third party.[61]

6.4. The rights of subjects

In terms of the rights of personal data subjects, the Regulation has exploited the rights originating from the directive, but brought in an already enhanced version, establishing them in a more detailed manner and recognizing additional rights.

Thus, the Regulation has affirmed once again the right to access to personal data that stems from the European Charter of Fundamental Rights.[62] However, aside from recognizing the right to have access to personal data, the Regulation also envisages the right of the data subject to obtain confirmation from the controller whether their data are being processed, about the purpose of the processing, the category of data subjected to these processes, the subjects where such data may be disseminated to, the period for which such data may be preserved, the right to obtain a copy of his/her personal data, etc.[63]

The rights envisaged in the Regulation have been enriched by recognizing greater control over personal data for data subjects as they may exploit the portability of data to another controller, based on their choice and assessment.[64]

Another novelty of the Regulation has to do with recognizing the right of the data subject to erase their data or, as consolidated by the CJEU practice, the right to be forgotten, in certain cases, for instance as when the data is no. longer important for the purpose they were collected for, or when the subject rescinds their consent about the processing of their data, when the data have been processed illegally, etc.[65]

6.5. Obligations of controllers and processors

The obligations of the controller and processor have been clarified by the Regulation by taking into consideration the problems that had arisen from the application in practice of the Directive. First, the controller is obliged to implement appropriate technical and organizational measures in order to be able to prove that the processing of personal data has been conducted in accordance with the requirements of the Regulation. These measures should be reviewed and updated every time necessary.[66] In other words, the burden of proof lies with the controller to prove before authorities the compliance of their activity with requirements of the regulation.

61 Article 6(1), GDPR.
62 Article 8(2), European Charter of Fundamental Rights
63 Article 15(1), GDPR.
64 Article 20, GDPR.
65 Article 17, GDPR.
66 Article 24, GDPR.

The Regulation has fulfilled the framework of obligations for the controller and processor with the task of drafting and implementing appropriate policies for the protection of personal data,[67] the obligation for transparency before subjects of personal data,[68] the obligation to integrate the technical projection of measures for the processing of personal data, "privacy by design" and "privacy by default,"[69] the obligation to maintain accurate records, similar to financial records, regarding the processing activity of personal data,[70] the creation of special structures within the controller body to cover personal data, the Personal Data Officer (PDO). This is an obligation of mainly public authorities or controllers whose part of main activity is the processing of personal data,[71]etc.

B. Regulatory Framework in the Council of Europe (CoE)

1. Convention for the Protection of Individuals Regarding the Automatic Processing of Personal Data

On the other hand, the CoE too has had added attention to personal data protection. Aside from what is envisioned in the European Human Rights Charter,[72] personal data protection has been enhanced also through other acts whose main target is personal data protection. We may mention here the Convention for the Protection of Individuals Regarding the Automatic Processing of Personal Data (known as Convention 108),[73] together with its protocols. The Convention represented an important act for two reasons: first, because it had a very broad reach (it was open for signing by countries that were members of the Council of Europe or not), thus aiming at creating as standard with as broad a basis as possible for the protection of personal data and, secondly, because it was the first international act that sought to protect individuals against abuse through processing of their personal data and create a regime for the transfer of such data. Convention 108 applies to all processing of personal data conducted by both the private and public sector such as processing by judicial or police authorities both from the public and private sector. In the same line as the provision of the Regulation, Convention 108 also has a double purpose: a) protection of personal data from illegal processing, and b) cross border circulation of personal data. Due to considerable technological development, the Convention has been modernized with a new protocol that responds to needs to adapt to technological developments (known as Convention 108+).[74] Given that the Convention does regulation at the level of principles, the Committee of Ministers has approved recommendations that seek to detail convention principles.

67 Article 24(2), GDPR
68 Article 12, GDPR.
69 Article 25, GDPR.
70 Article 30, GDPR
71 Articles 37-39, GDPR.
72 Article 8, ECHR (https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c)
73 Convention for the Protection of Individuals Regarding the Automatic Processing of Personal Data, Council of Europe, STCE no. 108, 1981. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108
74 Amending protocol to the Convention for the Protection of Individuals with Regard to the Processing of Personal Data, adopted by the Committee of Ministers at its 128th Session in Elsinore on 18 May 2018.

2. ECtHR Practice for Personal Data Protection

Aside from the Convention, the considerable caselaw of the ECtHR has also played an important role in the consolidation and sustainability of personal data protection. Its role has been particularly impactful in balancing the right to personal data protection and other rights, such as freedom of expression.

One of the issues that was subject of review in both courts (CJEU and the ECtHR) is that of Satakunnan Markkinapörssi Oy And Satamedia Oy V. Finland in which, the CJEU did not state whether the activity of the journalists in question (processing of publicly available data and the creation of an electronic database that might be accessed through telephone messages) could be deemed by domestic courts as representing journalistic activity or not.[75] Meanwhile, the ECtHR judged that the limitation of domestic courts on this activity (after the CJEU decision making, the domestic courts considered that this activity was a violation of personal data) was an expression of the balance that the state itself had established itself between freedom of expression and personal data protection within allowed margins. As a result, it did not represent a violation of freedom of expression.[76]

75 C-73/07, Tietosuojavaltuutettu against Satakunnan Markkinapörssi Oy and Satamedia Oy, 16 December 2008, para. 56, 61 and 62

76 Satakunnan Markkinapörssi Oy and Satamedia Oy V. Finland, Nr. Aplikimi nr. 931/13, p. 198 and 199

CHAPTER II

A. Albanian Legislation on Personal Data Protection

In Albania, the protection of personal data also has a constitutional origin and even is an autonomous right. Article 35 of the Constitution not only recognizes the right to personal data protection, but at the same time also guarantees some of the fundamental rights of the personal data subject. More concretely, article 35 establishes the right of the subject to allow personal data collection only through the consent of the person, the right to become familiar with data collected about the person, the right to seek correction or deletion of untrue or incomplete data, or those collected in violation of the law.[77]

Besides the constitutional framework, personal data protection has been completed through the ratification of Convention 108 and its different protocols.[78] At present, the changing protocol of Convention 108, known as Modernized Convention 108+[79] has been signed (on January 28, 2022 by Albania) and recently it was ratified in parliament.[80]

1. The Law "On Personal Data Protection" and the need for alignment

The acts mentioned above make a regulation with a principled approach and, in order to regulate the necessary technicalities and modalities, this framework has been completed by special legislation for personal data protection, through the approval of law no. 9887, dated 10.3.2008, "On personal data protection," amended. This law was approved at the time when the Directive for Personal Data Protection 94/46/EC was in force in the European Union; therefore, the law followed the model of the Directive. Clearly, due to the approval of an entirely new regime in the European Union for personal data protection, the law is not aligned with the General Data Protection Regulation.

Further on, we will be analyzing in a more detailed manner the need for alignment, assessing these acts from a comparative perspective regarding compliance of the law with the new standard established by the Regulation. In fact, the need for alignment comes not only as a response to the massive data breaches recently, but also as a repeated request of the European Union to harmonize this part of legislation. The Progress Report on Albania 2020 emphasizes that legislation on personal data protection needs to be aligned with Regulation 2016/679 and Police Directive 2016/680.[81] The 2021 report appreciates the efforts to realize alignment with European legislation in this regard, also based on the experience of the breaches of personal data of a sensitive character that included political preferences of individuals; therefore, there needs to be an update of the security level and limiting of access and use of personal data preserved in

77 Article 35, Constitution of the Republic of Albania: *"1. No one may be obliged, except when the law requires it, to make public the data connected with his person. 2. The collection, use and making public of data about a person is done with his consent, except for the cases provided by law. 3. Everyone has the right to become acquainted with data collected about him, except for the cases provided by law. 4. Everyone has the right to request the correction or expunging of untrue or incomplete data or data collected in violation of law."*

78 Law no. 9288, dated 7.10.2004, amended

79 https://www.idp.al/2022/01/28/28-janar-dita-e-mbrojtjes-se-te-dhenave-personale-2/.

80 Law No. 49/2022 "On the Ratification of the changing Protocol of the Convention for Protection of Individuals with Regard to the Automatic Processing of Personal Data."

81 Commission Staff Working Document, SWD(2020) 354 final, Albania 2020 Report, 6.10.2020, f. 30

state databases.[82]

The need to align legislation arises also due to an almost global standard that the Regulation establishes with regard to personal data protection. This standard is necessary in the context of the transfer of personal data as a need for economic development, as well as in the context of the principle of extra-territoriality that gives the Regulation effect also beyond the geographic boundaries of the EU if the data of individuals within the Union are processed by controllers headquartered outside the EU. Therefore, in this aspect, in order to recognize relevant obligations by controllers, it is necessary to create a similar legal framework that is in line with the obligations set by the Regulation.

2. Other important acts for Personal Data Protection

Aside from the law "On Personal Data Protection," other laws too have personal data protection as their purpose, although in more specific areas of activity. We may mention here the law "On electronic communications,[83] which, among others, establishes the rules for preserving confidentiality in electronic communications. In other words, these rules apply to all the information provided by the users of public communication networks, to protect from cookies and even viruses that represent another form of infringing upon the private life of the users of these communications. Regarding the protection of personal data, article 123(6)[84] that defines the obligation for the protection of users' personal data, is not fully harmonized with the Privacy Directive. This is the case because the field of application of article 5(3) of the above Directive is broader and it refers also to other ways of access to personal data of users (and external means through which information is preserved, such as CD, CD-ROM, USB, etc.),[85] besides the use of means of electronic communication. Data processing, according to the definition of the article in question, is allowed when the user or subscriber has granted consent, after they have been informed in a clear and understandable manner about the purpose of the processing. With regard to the way of obtaining consent, there is reference in the law "On personal data protection." In spite of lack of harmonization, what we see in practice also in the current situation is a marked lack of the implementation of this provision.

There is special regulation for state databases,[86] but this law does not contain any concrete regulation for personal data protection. Therefore, the reference to all aspects linked with the processing of these data shall be made in the law "On personal data protection." This means that the same legal standards and criteria of the LPDP shall serve to protect individuals from illegal actions in the field of personal data protection from public authorities.

In fact, even CMD no. 1147, dated 9.12.2020 "On the creation of the state database 'Unique Government Portal E-Albania' and the approval of regulations 'On the functioning of the Sole Contact Point,'" where a broad series of personal data of a general and sensitive character are stored, briefly establishes only the obligation for controllers to document the technical-organizational measures that have been adapted and implemented to guarantee personal data protection, aside from the general obligations that derive from

82 Commission Staff Working Document Albania 2021 Report, SWD (2021) 289 final 2021, f 27, 28
83 Law no. 9918, dated 19.5.2008 "On electronic communications," amended
84 Law no. 9918, dated 19.5.2008 "On electronic communications," amended
85 E. Kosta, Peeking into the Cookie Jar: The European Approach Towards the Regulation of Cookies, International Journal of Law and Information Technology (2013) 21(4), p. 380-406.
86 Law no. 10325, dated 23.9.2010, "On State Databases"

the law "On Personal Data Protection."[87] This CMD should have addressed carefully and with added attention the aspect of personal data protection from the Unique Government Portal, given that it is the portal where all citizens are obliged to provide personal data for.

3. Compliance of the Law "On Personal Data Protection" with the Regulation Standard

The Law "On Protection of Personal Data" was approved in 2008 and has been amended twice, by law no. 48/2012 and no. 120/2014 (referred to hereafter as the LPDP). The LPDP's focus is on two main subjects: the subject of personal data and the controller (and processor). The purpose of the norms included therein aims at protection of the rights of subjects against illegal processing of personal data and allowing, within the established boundaries, of their processing. The law's object is to establish the rules for the protection and legal processing of personal data.[88] In general terms, the law establishes rules for the protecting of personal data, the criteria for the legal processing of personal data, the transfer of data, the rights of subjects of data, obligations of controllers and processors, the Commissioner, also setting the Commissioner's competences and the part of sanctions applicable in case of failure to fulfill legal requirements. Beside the law, another important instrument in completing the framework for data protection have been the instructions issued by the Commissioner. In keeping with competences awarded by law, the Commissioner has concretized through regulations the rules for specific sectors in the field of personal data protection.

Among these, the following are to be pointed out: Instruction no. 47 "Setting regulations for preserving the safety of personal data processed by major processing subjects," Instruction no. 31 "Setting the conditions and criteria for exemption from the relevant obligations in processing personal data for journalistic, literary, or artistic purposes," Instruction no. 49 "On Protection of Personal Health Data," etc. However, we find that there an instruction on the access of electoral subjects to personal data is lacking.[89] In the aftermath of the massive data breach during the electoral campaign, it would be appropriate that the Commission, through an instruction, clearly establish the respective rights and obligations of the sides in this process. This instruction is seen as fundamentally important because personal data in an electoral context have added sensitivity not only for individuals, but also for the overall functioning of democracy. This is especially so to restore public trust in democratic processes.[90]

Further on, the analysis of the compliance of LPDP with the Regulation will be realized by looking at some of the main aspects, such as: area of implementation, rights of subjects, obligations of controllers, and implementation of provisions of the law.

3.1. Area of implementation

With regard to the material implementation, the law has stipulated that the norms seek the processing of personal data, fully or partially, through automatic means, and the processing with other means of personal data, which are kept in an archiving system or seek to form part of the archiving system.[91] In

87 Article 24, CMD no. 1147, dated 9.12.2020 "On the creation of the state database "Unique Government Portal E-Albania' and the approval of regulations "On the functioning of the Sole Contact Point.'"
88 Article 1, LPDP
89 Except for one implementation example according to Instruction 35.
90 Commission Guidance on the Application of Union Data Protection Law in the Electoral Context. An instrument spurred by the scandal of the illegal data processing by Cambridge Analytica, which created micro-targeting.
91 Article 4(1), LPDP

establishing the meaning of personal data, following the model of the Directive, the law has a more limited definition. Therefore, given that the Regulation has brought an expansion of the categories of personal data, especially sensitive ones, it is fitting that our law as well reflect that change. Thus, the Regulation adds to the definition of personal data also data that are linked with electronic activity such as location data or an online identifier, as well as expands the category of special data (known as sensitive data) to include biometric or genetical data for the purpose of identifying uniquely an individual and data about the sexual orientation of individuals.[92]

Regarding territorial implementation, the law stipulates that it applies to controllers in Albania, consular or diplomatic missions of the Albanian State, but also for controllers who are not located in Albania, but exercise their activity through means located in Albania.[93] Based on the way the provision has been formulated, it does not appear to have been aligned with the Regulation; therefore, given the standard created by the Regulation, it is important to establish also the implementation of the law in question for activities realized outside the territory of the Albanian state, but are linked with the processing of the data of individuals inside Albania. For instance, according to the Regulation, the controllers that track visited websites by individuals in the European Union will be the subject of the Regulation, although they are not headquartered inside the Union.

In this aspect, the law should follow the model of the Regulation and offer fuller protection for the rights of personal data subjects. According to the standard of the Regulation, the reach of the effect of the law to controllers or processors who are not in Albania, should be allowed in two circumstances: a) when the processing activity has to do with the provision of goods or services (with or without reward) to subjects of data in Albania, and b) when the behavior of persons inside the territory of Albania is monitored.[94]

Therefore, with regard to the field of material and territorial application, it is recommended that the law is updated according to provisions of the Regulation, in order to better protect the rights of data subjects, providing a broader definition of personal data, and extending its effect on controllers even beyond the territory of the Republic of Albania for activities that harm the interests of individuals operating inside the Albanian territory.

3.2. Legal processing of data

The legal processing of data, according to our law for personal data protection, is done in well-defined cases according to article 6 of the LPDP. The legal basis that allows for the processing of data acknowledges as causes: 1. The consent of the data subject; 2. When the processing is essential for fulfilling a contract; 3. For protecting the vital interests of the subject of data; 4. For fulfilling a legal obligation for controllers; 5. For carrying out a legal duty of public interest of the controller; 6. When the interest of the controller prevails over the interest of the data subject.[95]

The Regulation establishes the same causes that legitimize the processing of personal data, but some new substantial and procedural requirements have been defined regarding some of the causes mentioned above, which are not reflected in our law.

92 Article 4(1) and article 9(1), GDPR.
93 Neni 4(2), LPDP
94 Cf. article 3, GDPR.
95 Article 6(1), LPDP

First, regarding consent, for all categories of personal data, the LPDP does not have specific requirements regarding the criteria that the consent/approval should meet in order to be considered valid, aside from the definition of consent and the need to present it as a written statement and informing the subject on the need for the processing.[96] In this regard, the Regulation has established clearly some of the conditions for valid consent, which are: the possibility to withdraw,[97] is given freely, specifically, in an informed and clear manner.[98]

The criteria established above are important for guaranteeing the rights of subjects as, freely granting consent excludes the possibility of forced acceptance of cookies ore refusal of service (the take-it-or-leave-it option). Likewise, the need of the subject to provide informed and specific consent prohibits the use of requests for consent that are unclear and do not indicate directly the purpose of the processing. For instance, the request for processing data "for commercial purposes" is not sufficient and does not fulfill, in the sense of the Regulation, the conditions for the validity of the consent.[99]

Besides these conditions on the validity of the consent, the Regulation establishes other definitions about the protection of children, who should be at least 16 years old, in the context of online services. Moreover, the protection of children's rights has assumed added attention in the Regulation because the protection of the children's personal data may prevail even over the legal interest of the controller.[100]

In the spirit of these novelties, to be aligned, the LPDP should establish the conditions for the validity of consent and strengthen the protection of minors' personal data.

One of the other instances of allowing the processing of personal data has to do with the legal interest of the controller. However, this should be balanced with the interest of the personal data subject. In fact, the LPDP also has such a provision and requires balancing the interest of the controller with the fundamental rights of the data subject. However, this provision is inadequate for limiting eventual abuse by controllers. Therefore, following the same line as the Regulation, other requirements should be established on this cause. For instance, it may be notified by the controller of the legal interest and the protection of minors' rights.[101]

3.3. The rights of data subjects

In essence the rights of personal data subjects recognized by the LPDP are more or less the same as the regime of rights established by the Regulation. However, the latter elaborated some rights further and introduced some others, the path for which had been opened by the CJEU jurisprudence.

Thus, based on some of the rights that the Constitution recognizes for the personal data subject, the LPDP establishes that the subject shall have the right to access,[102] the right to block, correct, and delete,[103] the right to oppose,[104] the right to seek human intervention in automatic decision making,[105] as well as

96 Article 3 (24), LPDP
97 Article 7(3), GDPR. According to the Regulation, withdrawing consent should be as easy as giving consent.
98 Article 4(11), GDPR.
99 Ch. J., Hoofnagle et al, The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, 2019, Vol 28, No.1, 65-98.
100 Article 6(1), (f), GDPR, and article 8 GDPR.
101 Article 13(1)(d) and article 6(1)(f), GDPR.
102 Neni 12, LPDP
103 Article 12, LPDP
104 Article 15, LPDP
105 Article 14, LPDP

the right to complain.[106]

The Regulation not only recognizes and affirms these rights, but also elaborates them further, first by detailing them to create more guarantees for the data subjects, and by introducing some other new rights to grant the data subject more control, such as the right "to be forgotten"[107] as well as the possibility to take advantage of data portability.[108] Furthermore, the Regulation has detailed considerably the right of the data subject to be informed in a clear, simple, concise, and transparent manner about the controller, his/her identity and contact information, the way to contact the personal data officer, the purpose of the data processing, etc.[109] **In order to be aligned with the Regulation, the LPDP should expand and detail the rights of subjects in the spirit of the Regulation, envisaging also the right "to be forgotten" or data portability.**

3.4. Obligations of controllers and processors

One of the pillars on which the law bases personal data protection has to do with the establishment of a series of obligations for controllers and processors. The package of obligations that controllers have according to the LPDP includes: the obligation to inform,[110] the obligation to correct or delete,[111] the obligation to notify the Commissioner in case of processing of personal data,[112] and lastly, one of the most important obligations has to do with the undertaking of measures for the security of personal data[113] and protection of data confidentiality.[114] These obligations enable personal data protection, but do not guarantee the best possible protection. Breaches of data even of a sensitive nature dictate the need to add to the responsibilities and obligations for controllers.

In fact, the Regulation preceded this need as it not only affirmed the same obligations for the controller, but also expanded the scope of their obligations by shifting the oversight role of state authorities (i.e. authorities for personal data protection) to the controller himself.

3.4.1. Package of Obligations for Controllers Compared to the Standard of the Regulation

One of the novelties of the Regulation in terms of adding obligations for controllers has to do with their accountability. According to this requirement, the burden of proof to prove respect for the standards of the Regulation lies with the controller. The latter not only has to implement the requirements of the Regulation, but also be able to demonstrate that he has fulfilled all of the obligations deriving from the Regulation. Our law clearly recognizes the obligation of controllers to implement its requirements in automatic or other processing,[115] but in no case does it expressly require that the controller demonstrate and prove respect for the requirements of the law, except for when the Commissioner or even the court may request

106 Articles 16 and 17, LPDP
107 Article 17, GDPR.
108 Article 20, GDPR.
109 Article 13(1), GDPR
110 Article 18, LPDP
111 Article 19, LPDP
112 Article 21, LPDP
113 Article 27, LPDP
114 Article 28, LPDP
115 Article 5(2), LPDP.

this. According to the Regulation, controllers are obliged to prove compliance, among others, also on: a) obtaining approval (when required), according to Article 7(1), b) refusal of the request of the data subject for exercising the right to access or correction of data (article 11(2) and article 12(5)), c) non-respect for the right of the data subject to oppose the processing (article 21(1)), d) provision of guarantees and taking technical and organizational measures for the safety of data processing.[116]

Therefore, in this regard, it is necessary that the law also follow the same regime with regard to acknowledging the obligation of the controller to be accountable and task them with the burden of proof for compliance with all requirements of the law and not just the obligation to document technical-organizational measures according to article 27(2/1) of LPDP.

In this context, the Regulation has established the obligation of controllers to document clearly the entire processing activity. In fact, at present, the LPDP requires that the Commissioner is notified in advance about processing activity. However, this approach does not fulfill the purpose it was envisaged for, given that the Commissioner oversees a large number of controllers and the competence too review all notifications may appear unrealistic.[117] That was the reason why the Regulation changed its approach in this regard, avoiding the notification procedure and tasking the controllers to maintain data for all processing activity similar to financial balance sheets.[118]

Another obligation that the Regulation has added[119] that is not reflected in the current regulatory framework has to do with the obligation of the regulator to draft data protection policies, an obligation that aims at the controller being clear about the policy to be pursued with the personal data he collects. At present, our law on personal data protection is lacking an obligation of controllers to draft privacy policies.

One of the novelties brought by the Regulation regarding obligations of controllers was the obligation to incorporate protection in the technical design of services through data protection "by design" and "by default."[120] According to these obligations, controllers should adapt technological infrastructure by offering the options that guarantee maximal personal data protection. Both approaches seek to minimize the exposure of subjects' personal data. In Regulation terms, this obligation rests with the controller. At present, such an obligation is not reflected in the LPDP.

However, maybe one of the greatest obligations that will have to entirely change the approach of controllers toward the personal data protection process has to do with the creation of the Personal Data Officer (PDO).[121] In fact, state authorities for personal data protection cannot fully realize their purpose, especially in the circumstances of personal data processing activity that is constantly expanding. Therefore, the solution that the Regulation provided for this problem was through the creation of a new structure, entirely independent, whose function is to oversee the processing activity of the controller/processor so that this activity is realized in accordance with the requirements of the regulatory framework in force, i.e. the Regulation. In other words, the PDO will be the eyes and ears of the Authority on personal data protection on the controllers/processors. The role of the PDO is important for the exercise of internal

116 Douwe Korff and Marie Georges, The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, July 2019, p. 113-114.
117 Articles 21-25, LPDP
118 Ch. J., Hoofnagle et al, The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, 2019, Vol 28, No.1, 65-98.
119 Article 24(2), GDPR.
120 Article 25(1), GDPR.
121 Article 37-39, GDPR

control over compliance with the requirements of the law vis-à-vis the external control exercised by the competent authority for personal data protection. Already, the authority has a direct contact with a known person who represents the controller with regard to personal data protection and an auxiliary instrument for controlling the implementation of legal norms.[122] At the same time, the PDO will serve as a monitor of the evaluation of personal data impact and oversee its performance.[123]

In this regard, it is necessary that our legislation on personal data protection also establish such a structure in controllers in order to achieve a higher level of application of the norms for personal data protection. This new obligation for the controller will require staff that is trained about the law and in drafting manuals to assist the PDOs.

Another obligation established in the Regulation has to do with the drafting of the Personal Data Impact Evaluation in the case of data processing, which bears high risk with regard to the rights and freedoms of individuals. The drafting of impact evaluation is particularly required according to the Regulation in case of: a) systemic and expanded evaluation of personal aspects that is based on automated processing or profiling that leads decision making with considerable impact on individuals or that produce legal effects for them; b) processing at a large scale of personal data of special categories (sensitive data); c) systematic monitoring of a publicly accessible area, at a large scale.[124] The impact evaluation should address the reason for the data processing, the need and proportionality of the processing, as well as measures proposed to address potential risk, etc.[125]

The LPDP lacks such a provision so, in order to increase the level of compliance with the Regulation, the law on personal data protection should envisage such an obligation for the controller so that it may properly address the risks arising from processing activity that have an impact on a large number of individuals or when sensitive data is processed. The package of obligations for controllers, an obligation should be added that, in cases established by the Regulation, the impact evaluation be drafted.

Another obligation established by the Regulation has to do with the obligation for the implementation of adequate technical and organizational measures that respond to the proper level of potential risk, such as the pseudonymization and encryption of personal data, the possibility to ensure the confidentiality, integrity, availability, and continued sustainability of processing systems, the possibility to restore availability and access to personal data within a short time, in cases of physical or technical incidents, etc.[126] Presently, the LPDP contains a provision similar article 27, which requires the taking of technical-organizational measures by the controller; however, the Regulation has brought it to an updated format. From a substantial aspect, there is no difference, but to be in the same line as the Regulation, it should be adapted according to its spirit, identifying as main requirements of these measures the confidentiality, integrity, availability, and continued sustainability of the personal data processing system. clearly, the implementation of these measures requires additional costs for controllers, but certainly the implementation of the law costs less than its non-implementation.

122 Douwe Korff and Marie Georges, The DPO Handbook Guidance for Data Protection Officers in the Public and Quasi-Public Sectors on How to Ensure Compliance ëith the European Union General Data Protection Regulation, July 2019, p 120.
123 Article 39, GDPR.
124 Article 35(3), GDPR.
125 Article 35(7), GDPR.
126 Article 32 (1), GDPR.

Further on, the Regulation establishes that controllers have a double obligation to notify about cases of data breaches.[127] This means that cases of personal data breaches that lead to risk of fundamental rights and freedoms should be notified without delay, and when appropriate, not later than 72 hours after becoming aware of the fact. Aside from notifying the authority, the Regulation establishes also the obligation to notify personal data subjects in case the breach will pose a high risk to the rights and freedoms of individuals.

This obligation is lacking in the LPDP and that is why it is necessary to establish the obligation to notify in case of data breaches. This obligation, as established in the Regulation, should be two-sided, establishing also the obligation to notify data subjects when the data breach may threaten their rights or freedoms.

Lastly, the Regulation concludes the package of obligations for controllers with the obligation for collaboration and consultation. The obligation for consultation arises only in cases of data processing that may cause high risk to the rights of individuals, identifying this risk according to the impact assessment.[128] Meanwhile, the obligation for collaboration lies with the controllers and processors who, according to the request of the authority, is directed at fulfilling its duties.[129]

The obligation for prior consultation has not found room in the current law on personal data protection and, therefore, should be reflected in the LPDP. Meanwhile, the obligation for collaboration is an obligation recognized also by the LPDP and is directed at public and private institutions so that the CRIPDP may exercise the legally established functions.[130]

3.5. The Institutional Framework

3.5.1. Commissioner for the Right to Information and Personal Data Protection

The CRIPDP (referred to hereafter as the Commissioner) is the authority tasked by the LPDP to oversee implementation of the LPDP. The law acknowledges some rights of the Commissioner in the field of personal data protection, such as: a) conduct of the administrative investigation and the right to have access to personal data processing and collecting necessary information for carrying out his duties; b) ordering the deletion, blocking, destruction, or suspension of illegal processing of data; c) issuing instructions before the conduct of the processing and ensure their publication.[131]

In order to ensure the implementation of the law's provisions, the Commissioner has the right to issue recommendations[132] and, in cases of failure to implement them or cases of serious and repeated violations, publicly denounce and report the issue to the Assembly and the Council of Ministers.

The function of the Commissioner is very important for personal data protection and that is why the law has taken care to establish elements of independence, envisaging a 5-year term, with a right to re-election,[133] establishing the criteria for his/her selection,[134] clearly identifying cases of termination of the

127 Articles 33 and 34, GDPR.
128 Article 36, GDPR.
129 Article 31, GDPR.
130 Article 32, LPDP
131 Article 30(1), LPDP
132 Article 31, LPDP
133 Article 33, LPDP
134 Article 35, LPDP

mandate,[135] as well as recognizing the budgetary independence that may originate from donors without conflict of interest, aside from the state budget.[136]

In spite of such guarantees, just a reports and periodical reports of the Commissioner have highlighted progress, the Commissioner has not had full capacity in terms of human resources.[137] One of the deficiencies that has been highlighted and that plays an important role especially in the Information Technology and Communication sector is the lack of IT specialists.[138] In fact, the lack of staff has been highlighted as a deficiency in human resources for the Commissioner even by the annual 2021 report.[139]

Even in the European Union, authorities have often lacked the necessary staff and resources and often, they did not enjoy the necessary independence.[140] This is a fact proven even by the CJEU that some states have not preserved adequately the independence of authorities.[141] Therefore, the Regulation has aimed at strengthening the role of authorities in terms of their oversight activity. The Regulation has granted authorities powers for investigations, corrections, issuance of authorizations, and advisory activity.

In order to further strengthen the standing of the Commissioner, the law should specify and expand the competences of the Commissioner in the spirit of the Regulation. In this regard, duties of the Commissioner should be recognized legally for increasing public awareness and understanding about the risks, rules, guarantees, and rights with regard to processing, with a special focus on activities toward children, increase awareness of controllers and processors about obligations arising from the law on personal data protection, oversee developments that may have an impact on personal data protection, encourage the drafting of codes of conduct, etc.

With regard to investigative competences, the Commissioner's power should be recognized for issuing warnings on controllers and processors who will be engaged in processing activities that pose a risk for infringement of the rights of subjects protected by the Regulation, the opportunity to scold violators of norms of the law on personal data protection, order controllers and processors to respect obligations arising from the law, and order controllers/processors to notify data subjects in cases of personal data breaches.

Another competence for strengthening the standing of the Commissioner has to do with the right to start judicial processes for violations of provisions of the Law on personal data protection, a competence that the Commissioner now lacks.

3.5.2. Implementation of the Law

According to the LPDP, the authority for overseeing respect for provisions of the law is the Commissioner for the Right to Information and Personal Data Protection. In order to make the implementation of the norms of the law effective, a system of sanctions has been envisaged that varies from 10,000 leks up to 1,000,000 leks. The value of the fine is doubled for legal persons. Fines are imposed by the Commissioner depending on the type of obligation that has been violated.

135 Article 36, LPDP
136 Article 38, LPDP.
137 Albania Progress Report, 2021, p. 28.
138 Interview with Ms. Besa Tauzi, Director of Cabinet of the Commissioner
139 Annual Report 2021, Commissioner of the Right to Information and Personal Data Protection, p. 47.
140 Ch. J., Hoofnagle et al, The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, 2019, Vol 28, No.1, 65-98.
141 Seee C-288/12 Comission v Hungary ECLI:EU:C:2014:237, 8 April 2014.

As an alternative to the investment of the Commissioner and pursuit of the administrative path to complain about personal data breaches, the law also recognizes the possibility to pursue the case in the judiciary by filing a complaint, according to rules of the Civil Procedure Code in court. In fact, the provision has been formulated in an unclear manner and the damaged party may turn to the court directly, without being obliged to exhaust a complaint with the violator. The complaint with the violator envisaged by article 16(1) enables the resolution of the case through understanding, without investing the court, but is not an indispensable condition for filing the relevant lawsuit.[142] **Given that the provision allows room for double meaning, it should be clarified in the LPDP what the ways for complaining and the means available to the subject of the personal data. Regarding these possibilities of the personal data subject, the Regulation is clearer and envisages two possibilities for protecting the data subjects, such as a complaint with the relevant Authority and directly in court,** if it deems that his rights deriving from the Regulation have been violated by the activity of the controller and/or processor.[143]

In the European Union, the Regulation brought about a change also of the implementation regime as it recognized the possibility for filing class action and a root-deep change in the regime of fines. The preceding Directive was characterized by ineffective sanctions,[144] and that is why the Regulation changed its approach by aiming at the effective implementation of its provisions. The new system of administrative sanctions reflects a regime similar to applicable sanctions on the right to competition so that the Regulation would provide real protection for the data subjects. Therefore, for not-so-serious violations, the fines may vary up to 10 000 000 euros or, if the subject is an enterprise, the fine will be 2% of the total annual turnout of the preceding year,[145] and for more serious violations, the sanctions are doubled.

Also, the right to filing class action should also be recognized, recently confirmed also by the CJEU in case C-319/20, in which the court recognizes the possibility of Member States to allow associations for consumer protection to present representative actions[146] against the violation of personal data even without an authorization by the damaged subjects, that is independently, against the party responsible for the violation and infringement of personal data protection.

The approval of the law "On class action" may help implement these instruments also for personal data protection. Therefore, it is suggested that the sanctions regime in the LPDP should be adjusted according to the spirit of the Regulation. Maybe there will need to be a review of the country's economic development level, but the trend of fines should follow that of the Regulation.

Also, for as complete a protection of the data subjects and to facilitate their access to justice, in cases of massive data breaches, the possibility should be recognized for taking advantage of representative actions for protecting the interests of data subjects. In this regard, the approval of the law "On class action" will help.

142 Article 16, LPDP.
143 Article 79, GDPR
144 Ch. J., Hoofnagle et al, The European Union General Data Protection Regulation: What it is and what it means, Information and Communications Technology Law, 2019, Vol 28, No.1, 65-98.
145 Articles 83(4) and (5)
146 These are lawsuits filed by an organization in the name of one of the petitioners

3.6. Challenges in the implementation of the law

3.6.1. Challenges at the institutional level and practical implementation of the Regulation

The Regulation is still a new instrument that has set a good standard, at least in theory, for the protection of personal data. However, in spite of the short time for the full assessment of its effects, in the EU the instrument has been considered successful for achieving its main goals: 1. Protection of personal data of individuals, and, 2. Regulation of the circulation of personal data within the EU.[147] Some of the main conclusions resulting from the assessment of the Regulation two years after it went into effect have to do mainly with the institutional aspect of the authorities of member states that have the competence for personal data protection. With regard to the authorities, it has been stated that they need resources – human, technical, and financial – for the effective accomplishment of their duties.[148] Therefore, in a continued manner, the Commission has stressed the obligation of Member States to secure the necessary resources for state authorities for fulfilling their obligations according to the Regulation.

Aside from the institutional framework, the Regulation represents an interesting mixture between principles and concrete regulations so that these will act as an instrument that evolves and regulates even cases of technological developments that are not specifically addressed in the current version. The challenges that the Regulation may encounter in this regard have to do with the great amount of data processed (also known as big data), artificial intelligence, algorithms, blockchain technology, etc.[149]

Another challenge that the Regulation may encounter is fragmentation from domestic legislation, which should be drafted in almost the same manner to contribute to the uniformity of implementation and interpretation of the Regulation.

Based on the fact that the Regulation is a new act, it has been considered necessary that the European Board of Data Protection and state authorities issue guidelines and clarifications for controllers and processors.[150]

3.6.2. Challenges in LPDP implementation (even after alignment)

In Albania, the current challenges are mainly related to increasing awareness about personal data protection for the controllers and processors of such data and for citizens. Filling the needs for human, technical, and financial resources is another challenge linked with the implementation and exercise of the oversight functions of the Commissioner.

Legal changes will bring about an improvement in terms of clarifying the competences of the Commissioner and increased control of subjects over their own rights as well as added responsibilities and obligations for controllers. They will seek more staff for the Commissioner and better knowledge of the

147 Communication From the Commission to the Parliament and the Council, Data protection as a Pillar of citizens' empowerment and the EU's Approach to the digital transition- two years of application of the General Data Protection Regulation, SWD(2020)115 final, p.4.

148 Communication From the Commission to the Parliament and the Council, Data protection as a Pillar of citizens' empoëerment and the EU's Approach to the digital transition- two years of application of the General Data Protection Regulation, SWD (2020)115 final, p.6.

149 Council position and findings on the application on the application of the General data Protection Regulation, Brussels, 15 janar 2020, 14994/2/19, p.7.

150 Council position and findings on the application on the application of the General data Protection Regulation, Brussels, 15 janar 2020, 14994/2/19, p.6.

new duties and competences of this institution. Furthermore, another challenge that (maybe) even the new law on personal data protection will face has to do with technical development and changes brought about by artificial intelligence or blockchain technology. Therefore, added attention is needed from the Commissioner to follow these developments and evaluate the impact they have on personal data protection.

CHAPTER III

Efficacy of administrative and criminal investigation of massive breaches of personal data of voters, salaries of employees, and owners of vehicles

1. CRIPDP's Administrative Investigation

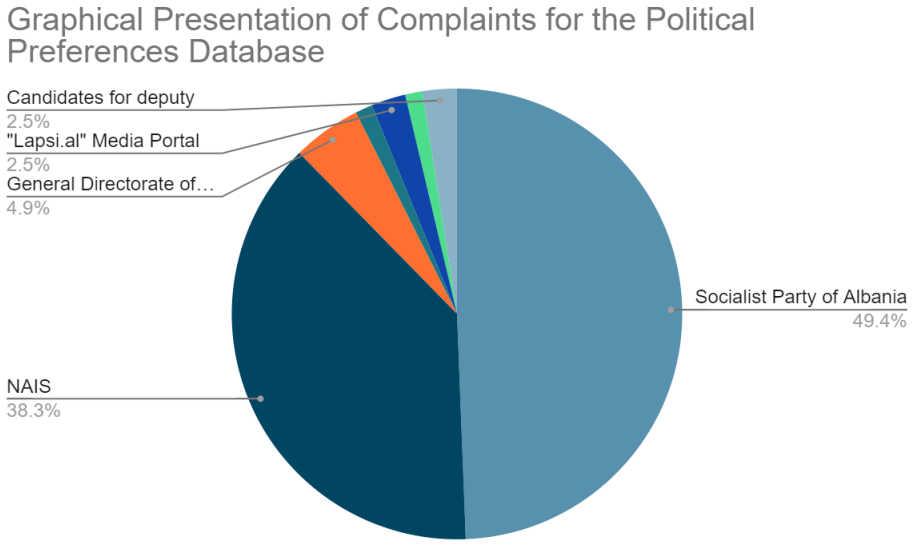
1.1 Citizens' complaints

According to article 16/1 of law no. 9887 on personal data protection, any person who claims that his/her rights, freedoms, and legal interests for personal data have been violated has the right to complain or notify the Commissioner and seek his intervention to reinstate the violated right. After this complaint, in keeping with the Civil Procedure Code, the subject of data may file a complaint in court. Article 16/2 envisages that if the data subject filed a complaint, the controller does not have the right to change the personal data until a final decision has been issued.

a. Voters' database

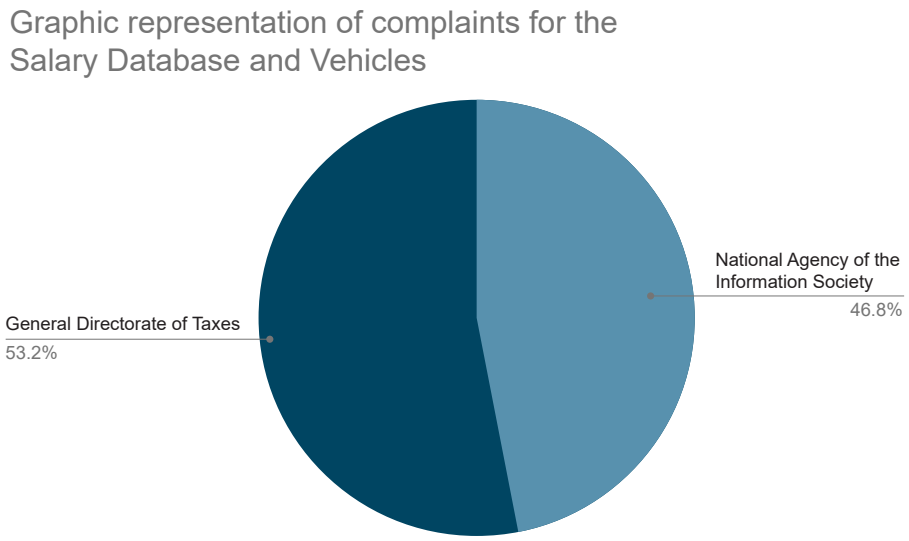
Based on the information that AHC has obtained, it notices that the Office of the Commissioner received 81 complaints during April – August 2021, which have to do with the verification of the lawfulness of the processing of personal data of citizens/voters. Although information was requested on the date of each of the complaints, this piece of information was not made available, which limits the evaluation of whether such complaints were submitted before or after the Commissioner began the administrative investigation on its own initiative.

Half of these complaints (49.4%) were filed against the electoral subject "Socialist Party" and, in an overwhelming majority, but less than half (38.3%), are attributed to the National Agency of Information Society (NAIS). The data are an indicator of the petitioners' perception on the responsibilities for this database. In a minority of the complaints, the subjects complained to the General Directory of Taxes, the news portal Lapsi.al, and candidates for MP.



b. Database of the salaries and vehicles

With regard to the illegal spread of the category of personal data for "officials/employees" in the public and private sector and the illegal dissemination of the category of personal data of "owners of vehicles," the Office of the Commissioner received 47 complaints, of which 22 against NAIS and 25 against the General Directory of Taxes. Although AHC sought information also on these complaints, including the data of these complaints, this information was not made available, which again limits the evaluation by AHC on whether these complaints were filed before the decision making of the Commissioner to start the administrative investigation by its initiative.



1.2 Start of the case by initiative

Based on article 30, paragraph 30, letter "a" of the law no. 9887 "On personal data protection" (amended), the CRIPDP conducts administrative investigation and has the right to access the processing of personal data, as well as collects all necessary information for fulfilling the oversight duties.

Given that the provisions regarding administrative investigation conducted by the Commissioner in the field of personal data are general, the rules, principles, and procedures that guide the administrative investigation of any public body, including the Office of the commissioner, are envisaged in law no. 44/2015, the "Administrative Procedure Code." The Code is a law approved by qualified majority and therefore its provisions prevail over provisions of laws approved by a simple majority. It is worth emphasizing that the reference to the Administrative Procedure Code has been realized by the Office of the Commissioner in the context of administrative investigations that began for the breaches of personal data with the databases that were circulated widely during 2021.

The principle of investigation by the initiative of the public body leads the section of administrative investigation, being envisaged in article 77 of the Administrative Procedure Code. According to this principle, the public body investigates by initiative all facts and assesses all the necessary circumstances for the resolution of the case. According to paragraph 2 of this article, the public body establishes, in an independent manner, the type, purpose, and reach of the administrative investigation, and assesses whether a fact or circumstance is necessary to resolve the case.

a. Voters' database

According to the Commissioner's letter no. 793/1, dated 22.04.2022, a letter of response, to the AHC and copies of orders made available, the institution began administrative investigation by its own initiative on "Verification regarding the lawfulness of the processing of personal data of citizens/voters." This investigation, according to the Office of the Commissioner began as soon as it was made known in the media that there had been an illegal spread of personal data for 910,000 citizens/voters. The administrative investigation appears to have begun on some controllers, for which, AHC was notified also on the Commissioner's relevant orders, as follows:

1. On the subject "Lapsi.al SHPK", administrative investigation started based on order no. 45, dated 19.04.2021.
2. On the subject "GDCR," the administrative investigation started based on order no. 46, dated 19.04.2021.
3. On the subject "NAIS", the administrative investigation started based on order no. 47, dated 19.04.2021.
4. On the subject "GDT", the administrative investigation started based on order no. 53, dated 29.04.2021.
5. On the subject "Socialist Party", the administrative investigation started based on order no. 57, dated 05.05.2021.

It is notable that although the date of the publication of the story in online media dates back to April 11, the first cycle of administrative investigation began 8 days late, namely on April 19, 2021, starting in an inconsistent manner chronologically on the inspected subjects.

On April 19, the Office of the Commissioner issued three separate orders on the conduct of the administrative investigation, on three controllers, namely the controller "Lapsi.al," the controller "General Directory of Civil Registry" and controller "National Agency of Information Society." Regarding the administrative investigation ordered on the controller that is a media subject "Lapsi.al," it is noticed that the Commissioner did not take into account the jurisprudence of the ECtHR on the importance of protecting journalistic sources, as a function of freedom of the press in a democratic society. The ECtHR notes that disclosure of the journalistic source may create the premises for limiting freedom of the press and free media.[151]

Eighteen days later, the Office of the Commissioner issued the order on the conduct of an administrative investigation on the General Directory of Taxes, while about 24 days later, the order included the last controller, the subject "SP."

It is unclear why the electoral subject that is suspected publicly in the media, the "SP," is last in the list of controllers to be investigated administratively by the Office of the Commissioner. This also applies to the fact that representatives of the subject stated within a short period of time that they manage a database, which they have created after years of organization, contacting voters door to door.[152] In such a situation, the urgency of verifying this massive data breach dictated an immediate need to carry out verifications at this electoral subject as well as in the public entities that are in contact with information similar to what the database contained (such as, personal numbers, places of residence, workplaces, etc.). This urgency was also dictated by the need to immediately secure evidence in the computer systems of these subjects so that such evidence would not be manipulated or damaged.

151 https://www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf

152 https://lapsi.al/2021/04/11/alibia-e-taulant-balles-per-pergjimin-qe-ps-u-ben-te-dhenave-personale-te-qytetareve/ https://lapsi.al/2021/04/13/rama-pranon-patronazhistet-kemi-vite-qe-i-kemi-shperndare-ne-terren/

b. Database of salaries and vehicles

Unlike in the case of starting the investigation on its own initiative for the voters' database, the start of the administrative proceedings on the salary database began immediately after the publication. This is certified by the order of the Commissioner no. 203, dated 22.12.2021, which orders the administrative investigation on the controller "General Directory of Taxes."

Regarding the database of the vehicle owners, the start of the first administrative investigation dates to December 28, or four days after the story was published and it was ordered on the controller "General Directory of Road Transport Services."

The Commissioner began administrative investigation into these two databases on the subject "NAIS," namely on February 25, 2022, or about two months after the date when the news of its existence was published.

It is worth emphasizing that both, for the salary database and the vehicles' database, the Office of the Commissioner did not order administrative investigations at the media outlets that made public the news of their existence. In this regard, the intermediate ECtHR decision in favor of applicants administering the media portal "Lapsi.al" may have had a positive impact.

1.3 Target of the Administrative Investigation

The Office of the Commissioner considers the massive personal data breach as a *"personal data breach"* (referring to the international legal terminology), investigated administratively in three cases on:

a. Illegal dissemination of data of the category citizens/voters;
b. Illegal dissemination of data of the category "officials/employees" in the public and private sector;
c. Illegal dissemination of data of the category "vehicle owners."

The target of these three administrative investigations coincides and began chronologically during 2021, following the publication of news about the existence of the databases.

1.4 Means of seeking evidence and the efficacy of the administrative investigation on the inspected subjects

As stressed earlier, Law no. 9887, dated 10.3.2008 "On personal data protection" envisages the competence of the Commissioner in the field of protecting personal data for conducting administrative investigations and having the right to access the processing of personal data, as well as the right to collect all necessary information for carrying out the oversight duties.

For the purpose of administrative investigations, article 80 of the Administrative Procedure Code envisages the understanding and means of seeking evidence. According to paragraph 1 of this article, in order to establish the state of facts and circumstances that have to do with the case, the public body may:

a) collect statements from the parties, witnesses, and experts;
b) obtain documents and other documents that have been documented through photographic means, registration, or other technical means;
c) visit and check goods or involved locations.

In paragraph 2 of this article, the Administrative Procedure Code expands even further the concept of seeking evidence that is available to the public body, making a reference to the provisions of the law on the organization and functioning of administrative courts and the resolution of administrative disputes, which are implemented, as long as it is possible in the administrative procedure, except for when envisaged otherwise in this Code.

Article 86 of the Administrative Procedure Code also grants the public body the procedural guarantee to secure evidence, when noticing that obtaining a piece of evidence is at risk and if the resolution of the case depends on that evidence or the evidence impacts its clarification.[153] Due to the importance of obtaining evidence in a timely manner, paragraph 2 of this article envisages the guarantee to secure evidence even before the administrative procedure has begun.

Looking at the documentation provided by the Commissioner regarding the administrative investigation into these three databases, we notice that the investigation orders on the controllers do not clearly and fully establish the elements envisaged in article 77, paragraph 2 of the Administrative Procedure Code. Concretely, this article requires that the public body establish independently the type, purpose, and scope of the investigation, Commissioner's orders:

- envisage the determination of the inspection team, which is authorized to conduct procedural actions for conducting the inspection, implementing legal requirements for this purpose;
- establish the purpose of the investigation, in accordance with article 77, paragraph 2, to verify lawfulness of the processing of personal data of citizens/voters;
- do not provide guidance on the procedural actions that will be conducted by the inspectors or the means for seeking evidence that will be implemented and how far the concrete investigations will reach on each controller;
- are standard in content and do not take into consideration the nature of the activity of each controller, the sector the subject (public or private) represents, the data that are or that may be administered by it, and other specifics of the controllers.

The individualization of the investigative activity would be essential because it would need to be assessed whether a fact or circumstance is necessary for resolving the case, which should be determined from the very start of the administrative investigation (article 77, paragraph 2, of the Code).

1.4.1 Enhanced analysis of the report of the Commissioner's Office on the administrative investigation of the voters' database

The Commissioner stated in its responses that the findings evidenced for the administrative investigations of the first database were addressed in the Report on the Administrative Investigation on the illegal dissemination of citizens' personal data, prot. No. 1399, dated 19.08.2021, which is published on the official website of the Office of the Commissioner.[154]

153 When this evidence is at risk of disappearing or becoming difficult or obtaining it becomes impossible. Securing the evidence or otherwise known as taking it in advance may be done by the public body, on its initiative or by the justified request of the party

154 https://www.idp.al/wp-content/uploads/2021/09/Relacion_hetimi_administrative_per_perhapjen_e_paligjshme_te_te_dhenave_personale_t e_shtetasve.pdf

In the spirit of constructive criticism, the systematic analysis based on legal standards on the report on the administrative investigation of the Office of the Commissioner features the following deficiencies:

- The investigation appears to have been conducted partially and in a shallow manner, while the Office of the Commissioner could have taken other necessary measures to seek a greater diversity of evidence that make it possible to resolve the case and concretely identify the responsibility of controllers.
- Seeking information from the investigated subjects, namely the GDP and SP, was done late, namely 20 and 40 days after the start of the investigation on them. this delay weakened the administrative investigation in a reasonable time and with efficiency, and it may have influenced the alteration or hiding of necessary evidence, which the Office of the Commissioner did not seek to secure at the start of the administrative investigation (such as the servers or other sources of evidence).
- The report does not reflect the concrete procedural actions that were undertaken by the inspection team in the inspection at the subjects while added attention has been devoted to the reference and broad interpretation of the law on personal data and previous instructions of the Commissioner.
- During the investigation at the subjects, the Commissioner presented a list of questions and requests regarding the processing activity of personal data by each inspected subject. Except for the GDCR, the 3 other controllers showed a low level of collaboration in providing information and accepting responsibility. It is a notable fact that this information was not confronted by the Office of the Commissioner to other information that might have been obtained during the administrative investigation, which raises questions on the access of inspectors to the computer systems and servers of the inspected subjects.
- The Office of the Commissioner did not display a proactive approach in issuing administrative sanctions by a fine for violation of article 2 of law no. 9887/2008 on the subjects that underwent the administrative inspection and did not collaborate adequately to make information available. In fact, an administrative sanction was only issued on the GDP, 4 months after the administrative investigation began, while in such a situation, the reaction could have been immediate after the lack of information and access to computer systems for each of the inspected subjects.
- Although all of the major controllers have the obligation to create, administer, and maintain the Information Security Management System (ISMS), this system appeared lacking in almost all the state administration institutions that the NAIS investigated administratively. This data was reflected also in the annual reports of the CRIPDP to the Assembly for 2021. Nevertheless, this signaling by the CRIPDP did not help prevent the incident.
- At the conclusion of the administrative investigation on the three subjects (public controllers), the office of CRIPDP reaches hypothetical conclusions that the possibility may not be ruled out that the data in the canvassers' database may have been taken from the database controlled and/or processed by these institutions or subjects that are contracted or sub-contracted by them. Such conclusions do not serve public interest or the responsibility of institutions while they again highlight the indispensability of enhancing the administrative investigation and exhausting all means for seeking evidence in accordance with law no. 9887/2008 and the Administrative Procedure Code.

i. Administrative Investigation at the GDCR

Based on verifications by the Office of the Commissioner at the GDCR, 30% of the voters' database consists of data that originally the GDRC conveys to electoral subjects according to article 60 of the Electoral Code.[155] The same electoral components from the data processed by the GRDC may be accessed by the concessionary company ALEAT, the General Directory of the State Police (GDSP) and NAIS.

It is a notable fact that in reference to the joint instruction no. 463, dated 10.12.2020, of the Commissioner and the Minister of Interior, it results that there are 36 other controllers who have access to these data, according to the relevant legal rights and obligations. Referring to the register of services of provider-consumer databases, administered by NAIS, it results that there are 47 public/private institutions that have access to the National Civil Registry (NCR).

A disturbing problem that the Office of the Commissioner has encountered since 2019 in controller GDCR and later, on April 9, 2021 (two days before the publication of the database) addressed NAIS, GDCR, and the GDSP, has to do with the request to block and start legal proceedings on persons/subjects who are behind the public website https://gjendjacivile.bogspot.com/p/falas.html.

This internet website continued the publication of personal data obtained from the NCR, updated until 2008. Upon recommendation no. 26 of 2019, the Office of the Commissioner left a series of tasks to be carried out by the GDCR and asked AEPC in the same year to block the internet website.[156]

The Office of the Commissioner notes that for part of citizens whose data were processed in the Voters' Database, they are accessible illegally also on the above website. **As a function of transparency and accountability to the public, the latter should have been informed why since April 2019 and two years after, the recommendations of the Office of the Commissioner were not implemented? Could a potential massive breach be avoided by these sources if the principle of administrative responsibility had been implemented, in accordance with sanctions envisaged by the law in force on personal data?**

The Office of the Commissioner states that procedural actions have been conducted at the GDCR that involve statement of findings on site and review of the legal basis and internal acts. This explanation is inadequate in the sense of alternatives of means of seeking evidence as envisaged in article 80 of the Administrative Procedure Code. Such evidence could have been secured by statements by the parties, witnesses and experts, documents, including those secured by photographic, recording, or other technical means, etc.

The GDCR states that article 60 of the Electoral Code envisages making available to electoral subjects and/or political parties the voter lists and extract of electoral components. Such documentation may be made available also electronically, which is done in such a form that allow searchers and cross comparisons. However, in spite of the legal arguments of the GDCR, we find that the report of the Commissioner does not clarify on what date the lists/extracts were made available to the electoral subject that is suspected in the media and whether such data coincide with the database of voters and the database that the SP electoral subject secured in its own servers and information technology systems.

The GDCR states that there are 590 active users who have access to the graphic interface of the civil registry system user. Users at the database level, with reading/updating rights, among other things, guarantee

155 Personal data (electoral components) that the GDCR conveys to electoral subjects include concretely the name, father's name, family name, date of birth, personal number, and citizenship.

156 See page 18 of the Report on the Office of the Commissioner's Administrative Investigation

backed-up copies of the database, preserving them in the dedicated back-up equipment. The report does not clarify whether the inspectors conducted verifications in the dedicated back-up equipment and whether there were transfers of back-up copies to unauthorized persons or equipment.

To the question of the Office of the Commissioner to list third parties that personal data are transmitted to, the GDCR responded by citing instruction no. 463, dated 10.12.2020,157 according to which it results that there are 36 controllers who access data from the NCR. The government interaction platform that is managed by NAIS makes it possible to exchange data with third parties, to avoid dissemination of personal data by them. It is worth noting that in its report, the Office of the Commissioner does not argue the lack of expanding administrative investigations also on these 36 controllers, which would contribute to as comprehensive as possible investigations to resolve the incident.

Also, the report says that there is a low match of the categories of data processed by this controller (GDCR) compared to those reflected in the Voters Database, and this is one of the indicators that makes it impossible to prove that whether this database was populated with NCR data. However, the fact that 30% of the NCR data or 6 of 20 pieces of data) are part of the voters' database represents a sufficient level that cannot exclude the responsibility of the GDCR or controllers who have access to such data, for their breach. It is notable that in this conclusion, the office of the Commissioner is based also on findings on site by the group of inspectors that are not quoted even in a summarized manner as to what the data obtained by them consisted in.

ii. Administrative Investigation at the GDT

The report states that the Office of the Commissioner has conducted an administrative investigation at the GDT, where the inspection group sought information and clarifications regarding processing processes, categories of data, data subjects, etc.

From April 19, which coincides with the start of the administrative investigation by the Office of the Commissioner on the GDT, information by the latter was made available electronically 21 days late. This delay weakens the administrative investigation within a reasonable time and with efficiency. Moreover, although it took a relatively long time, it is disturbing that the GDCR has not been collaborative in providing information and denied its role as a "controller" for the data.

Part of the missing information from the GDT that could have helped the administrative investigation is the one with the logs and traceability of logs for access to the system. the GDT states that, *"Logs, the traceability of logs for access to systems should be requested case by case according to the target of the investigation and will be made available if they are not information that has been classified as 'state secret,' which is made available only after fulfilling all the criteria of legislation in force."*

It is a disturbing fact that the GDT did not recognize the attributes of the Commissioner according to law no. 9887/2008, article 31/1, letter "ç", to become familiar with and have access to information and documents that are the target of the complaint, according to the law on the right to information or that are linked with the case under review, including information that is classified as "state secret."

The obligation for public and private institutions to collaborate with the Commissioner has been envisaged expressly in article 32 of law no. 9887/2008, whereby paragraph 2 envisages that the Commissioner has access to the computer system, archiving system, that conduct processing of personal data and to all

157 Joint one of the CRIPDP and the Minister of Interior.

documentation that is linked with their processing and transfer, for the exercise of the rights and duties assigned by law.

Although the GDT displayed in the first 20 days of the administrative investigation a non-collaborative behavior, the Commissioner decided to issue a fine of 1,000,000 leks on August 23, that is three months and a half later.[158] In an issue that has high public interest, when the obligations of legislation on personal data protection are not acknowledged or respected by an public institution such as the GDT and when the non-collaborative approach is displayed from the start of the administrative investigation, the sanction should have been imposed within as reasonable time as possible, as a function of the principle of responsibility before the law and the efficacy of the administrative investigation. In our opinion, the Commissioner could have taken legal escalated and proportional steps to have access to this information, in as fast a time as possible and pursuant to legal sanctions in case of lack of collaboration.

The problems related to preservation, protection, and security of personal data during processing processes conducted by the GDT were stated by the CRIPDP in an inspection of 5 months earlier that was not related to the target of the administrative investigation of the voters' database. These problems were reflected in the annual report to the Assembly on February 8, 2021, and have to do with the lack of a specific regulatory framework of the GDT in this field, the lack of standardized and periodical monitoring processes for preserving the integrity of data, etc. However, it is to be noted that these findings were only left at the level of recommendations for the GDT while no sanctions were issued according to article 39 of law no. 9887/2008. We bring to attention the fact that according to paragraph 1, letter "dh" of this article, controllers or processors who do not take measures for data security and do not implement the obligation for preserving confidentiality are fined with 10,000 up to 150,000 leks, an amount that is doubled if committed by legal entities.

iii. Administrative Investigation at NAIS

Even for this subject, the report of the Commissioner's Office states that it conducted an administrative investigation and the inspection team sought information and clarifications regarding the processing processes, categories of data, data subjects, etc.

Besides the need to individualize the administrative investigation vis-à-vis the specific competences of NAIS, it is our opinion that the target of the investigation could have been more direct, to verify whether there were data transfers from the computer systems of NAIS on unauthorized persons/subjects and equipment, whether that transfer is enabled by the computer and security system administered by NAIS, when the last inspection on security regulations was done, etc.

In its responses, NAIS does not display a good collaborative conduct for providing information to the Office of the Commissioner, also denying its controlling and processing role on data. Furthermore, the NAIS states that it does not disseminate data because it does not have access to them. Regarding the request of the Commissioner's Office to make available the list of institutions that this subject provides technical assistance to and the category of data accessed by each of them, the NAIS does not respond clearly with concrete responses.

158 See decision no. 807/4, dated 23.08.2021, published at this link: https://www.idp.al/wp- content/uploads/2021/08/vendimi_nr_41_dmdp_2021.pdf

It is notable that part of the responses by NAIS that avoid giving information are the same as the responses of the GDT, thus raising questions about the interaction and exchange of information between these institutions, during the CRIPDP's administrative investigation. Thus, to the CRIPDP's question on the contracts for system maintenance, the NAIS responds like the GDT, that they should be requested on a case-by-case basis, depending on the target of the investigation.

In the part of its findings, the CRIPDP states that the administrative investigation at NAIS was realized based on documentation made available by this controller and its responses on the questions/requests submitted in the context of the investigation plan. This finding highlights that the CRIPDP inspectors did not have access to the servers, computer systems, archiving and security systems that the NAIS administers while this is the key institution that manages the government interaction platform.[159]

In order to oppose the non-agreeing approach of the NAIS as a controller, processor, and not accessor of data, the CRIPDP lists and argues in a detailed manner the competences of this subject according to CMD no. 673. Among these is the possibility to exchange data of electronic systems, through the government interaction platform, in accordance with security terms.

The Office of the Commissioner admits that the responses of NAIS regarding its capacity as a controller/processor, and access to data, appear to be non-exhaustive and do not help the process of the administrative investigation. This statement applies also to the failure to address requests submitted at some points in the investigation plan. Furthermore, the CRIPDP finds that the NAIS, in its capacity as co-controller of data, is obliged to respond to fulfill the obligations deriving from legislation on personal data protection.[160] However, in spite of this finding, the lacking or limited responses of the NAIS to CRIPDP requests were not sufficient for the latter to issue administrative punishment for violation of article 32 of the law no. 9887/2008. This approach of not applying sanctions reflects a standard that is not the same by the CRIPDP as in the case of the subject investigated on the same case, the GDT.

Based on Instruction on. 47 of the Commissioner, all major controllers (including the NAIS) have the obligation to create, administer, and maintain the ISMSs for the protection of personal data. In almost all state administration institutions, including the NAIS, which were inspected on the basis of the order of 09.11.2020 by the Office of the Commissioner, inspectors found the ISMSs lacking. The problem was reflected in the annual report of the CRIPDP for 2020 before parliament. Among others, the report notes that the NAIS does not include in its organizational structure an independent function for monitoring and improving this system continually, which would play an important role in information security and efficacy of the ISMS.

At the end of the report,[161] the Office of the Commissioner does not exclude the possibility that the Database was populated by data controlled and/or processed by the institutions that are the target of this investigation or contracted/subcontracted by them. The CRIPDP notes that the breach may be a result of the lack of security measures by subjects that have the right to access such data, or the institutions where such data are primary and/or secondary data in databases created according to legislation in force. This hypothetical conclusion on the NAIS and other subjects in the public sector displays the lack of a complete and comprehensive administrative investigation, according to law no. 9887/2008 and the Administrative Procedure Code.

159 See page 14 and 26 of the Report.
160 See page 30 of the Report.
161 See p. 34 of the Report

iv. Administrative investigation at the subject "Socialist Party" (SP)

News of the existence of the database was made public on April 11, but the administrative investigation on the electoral subject suspected of creating it began about one month later, on May 5, 2021. Aside from being late in starting investigations, even the subject's reaction to make available requested information during the inspection on site by the CRIPDP inspectors was late, precisely on Jun 14, or two months after the publication of the news. It is unclear from the contents of the report why this information was obtained so late and whether there were prior inspection visits in the field, to the offices of the electoral subject.

The database of canvassers for Tirana Municipality dictated the need for the inspection to extend to all offices of the electoral subject located in this Municipality.

Moreover, obtaining information took a relatively long time, the electoral subject was not fully collaborative in providing it. As noted in the report, the controller in question did not provide concrete information on what are the physical and technical security measures of self-administered systems, contracts and rapport with system maintenance providers, how data subjects' rights are guaranteed, whether there were requests by data subjects to delete personal data, and fulfilling duties in the capacity of the controller.[162] Nevertheless, the lacking or partial responses of the subject to CRIPDP requests were not sufficient for applying administrative punishment for violation of article 32 of law no. 9887/2008.

Referring to the statements of representatives of the subject, the findings on site by CRIPDP inspectors, and data of the online interface of the voters' list possessed by the SP, it results that this controller possesses two categories of data, namely party members and data of the voter lists.

The CRIPDP report does not provide any information what means were used for seeking evidence to obtain data during the inspectors' visit to this subject. The report does not provide information on whether the group of inspectors accessed initially the inventory of equipment owned and administered by the electoral subject, thus raising questions about failure to realize verifications in computer equipment that serve to process personal data. The CRIPDP highlights in its report that the server where the database where the of data accessed through the online web interface is installed locally, in the headquarters of the controller, but there is no information on whether this server was subjected to inspection and verifications and the findings on site by inspectors about it.

The report states that the representatives of the electoral subject declare that the categories of voters' data were obtained from the CEC, upon request of the legal representative of the SP, embedded with this institution.[163] However, it is unclear when these data were obtained for the last time, whether they correspond in terms of accuracy to that category of data that are part of the NCR with the database administered by the electoral subject. Specifying the date/s of obtaining the voter lists and the cross checking of information fully and not just based on the matching categories would have served the comprehensive administrative investigation to prove or exclude the claim of the subject that data was obtained from the NCR.

Two data categories that were added (different from those in the NCR) are the phone number and the data on political preferences (census), which, according to the electoral subject were added by the canvasser. Such data, according to the subject, were collected through the canvassing system, based on internal instructions on January 11, 2021, which coincides timewise to 3 months before the publication of the news on the database. The canvassing system consists of party members and sympathizers who have

162 See p. 36 of the Report.
163 See page 38 of the Report

been made available the voter list and their task is to conclude the census (highlight the voter's preferred political party and maintain contact with voters under patronage, until the voting concludes).

Based on the contents of the CRIPDP report, there is some lack of clarity on the functioning of the canvassing system, on the following, among others:

- in what way were the voters' contacts and preferences obtained, transferred, administered, and processed;
- have the voters contacted by the canvasser granted approval for the transfer and processing of such data, and how was their consent documented,
- how was the procedure organized for inputting, administering, and processing the data in the database of the electoral subject, who is responsible, etc.

Further on, the report explains that the subject's official website enabled a mechanism that *a priori* collects personal data without the expressed consent of the data individual (referring to the section "recommend your friend"), but this finding does not shed light on the canvassing mechanism regarding the contact canvasser-voter, as highlighted above and whether the requirements of law no. 9887/2008 on obtaining, transferring, and processing of data, are respected.

The focus of the Commissioner's investigation has been expanded beyond the target because the report analyzes not only data obtained with the canvassing system for voters, but also data about the members of the electoral subject. The report of the Commissioner draws a comparison between the membership form and the database of voters circulated via the WhatsApp application, while the main target of the investigation should have been how voters' data, obtained through the canvassing system, were obtained.

Furthermore, it is noticed that the Commissioner did not conduct complete verifications on the 81 complaints submitted by citizens to the subject, whether their personal and sensitive data were featured in the SP computer system, secured through the canvassing system. Such verifications could have been expanded beyond the petitioners" category, to cover a certain sample of voters who are overseen by canvassers, referring to data that the subject administers (whether they were made available to the Commissioner).

The CRIPDP does not exclude the possibility that the Database was created and used by local levels of political-electoral organization and/or bodies or structures of specific candidates (or subjects contracted/subcontracted by them), in violation even of the internal rules for the organization of this Controller.[164] This conclusion of the CRIPDP relies on incomplete facts, which in our opinion should have been investigated fully and comprehensively. This thesis is not convincing in the eyes of public opinion and bears elements of biased subjectivity that minimizes the responsibility of the electoral subject as a major political organization.

In the absence of a complete and comprehensive investigation, there are elements of subjectivity for an external observer even the finding that "the lack of existence of a database, similar to the database, in no other territory of the political organization of the SPA in the country exempts this controller from the suspicion of having authorship in the creation and administration of the database." It is unclear whether this conclusion was the product of verifications conducted in every territorial unit where the subject has its offices or only on the statements of the subject's representatives.

164 Page 40 of the report.

The report further notes that the SP, as a large processing subject, has not created the information security management system (ISMS) for the protection of personal data, as envisaged by Instruction no. 47 of the Commissioner.[165]

v. Conclusions and difficulties highlighted during the investigations

The Commissioner considers that the facts and circumstances of the administrative investigation do not create the conditions to highlight and prove, in concrete investigative terms and steps, the creation and use of the database by any subject of administrative investigation.

The conclusions and recommendations reflected in parge 42 of the report of the Commissioner highlight the great complexity of the issue under investigation, the dissemination of the database to an indefinite number of receivers, as well as the lack of sufficient technical and human resources and capacities to address a data breach of such dimensions, which does not make it possible to identify the source of the creation, administration, and dissemination of the Database.

For the sake of transparency and accountability, it would have been worth mentioning in the report what the sources (human and technical) were that the Commissioner had available for carrying out the administrative investigation, whether the objective possibilities existed to overcome the difficulties by contracting external experts and the necessary technical equipment that would enable the administrative investigation in as complete, comprehensive, and objective manner as possible.

It is our opinion that in the face of such an emergency of the massive breach and exchange of personal and sensitive data, the CRIPDP should have devoted proper attention to all possible solutions, including a request to the Assembly about the needs regarding the Commissioner's budget that would enable the application of these solutions.

In the official response to AHC, the CRIPDP highlights as difficulties the non-efficacious coordination with the prosecution office to continue quickly the administrative investigation. According to the CRIPDP, the evidence, which includes servers or computers at the controllers under administrative investigation by the Commissioner were initially placed under sequestration by the prosecution office. Regarding this matter, AHC notes that such information is contradictory compared to those from the prosecution office, according to which the decision for sequestration appears to be in the context of the criminal investigation on the salary database and not on the voters' database. According to the prosecution office, the computers owned by citizens A.A. and E.Q. and the hard disk of citizen K.S. were sequestered.

However, it is worth highlighting that the special prosecution office did not provide information about the criminal investigations conducted by it and whether there were sequestrations on computers or servers of the 4 subjects that the Commissioner investigated administratively (GDCR, GDT, NAIS, and SP).

It is unclear whether there was correspondence or communication between the prosecution body and the CRIPDP on the investigations they conduct and steps suggested to overcome it. **In any event, the lack of access to computer networks and systems, to archiving systems or servers of the four subjects may not be justified by the fact that the prosecution office imposed sequestration measures, first, because the administrative report should have highlighted which of these equipment or computer data was sequestered, whether the sequestration was definite, and whether this fact obstructed verifications and access of the CRIPDP to equipment and computer systems that were not under prosecution's sequestration.** Another

165 Page 42 of the report

way to avoid this obstacle before making a final decision would be to suspend the administrative proceedings until the obstacle to the public body (CRIPDP) ceased to exist.[166]

1.5 Timespan of the investigations

Law no. 9887/2008 on personal data protection does not envisage deadlines for administrative proceedings conducted by the CRIPDP on issues in the area of personal data protection. In the absence of such provisions, the legal reference on deadlines is that in article 49 of the Administrative Procedure Code, according to which the administrative proceeding concludes within a 3-month period.[167]

According to the letter of the Commissioner, the timespan of the administrative investigation by its own initiative on the illegal dissemination of the category of citizens/voters' data lasted about 4 months, with the end being the date of publication of recommendations for the investigated controllers.[168]

With regard to the administrative investigation process on the illegal spread of the category of data on "officials/employees" in the public and private sector and vehicle owners, as mentioned above, the investigation was ongoing while this analysis was being conducted. Therefore, any further development regarding the progress of this case is not included in the analysis featured in this document.

1.6 Recommendations of the Commissioner on the subjects that were administratively investigated

Pursuant to article 39 of law no. 9887/2008, in cases of processing of data in contravention of the provisions of this law, when they are not a criminal offense but are an administrative offense, the Commissioner imposes a fine that varies between 10,000 leks and 1,000,000 leks, depending on the legal obligation violated by the controller or processor. When the offense in personal data is committed by legal entities, they are fined double the amount according to the violations and level of fine envisaged in paragraph 1 of article 39.

Until April 11, 2022, which corresponds to the official response of the Commissioner to AHC, it results that the administrative investigation into the database on the lawfulness of processing of personal data of citizens/voters has been concluded. In the context of this investigation, the Commissioner found administrative violations punishable by a fine of 1,000,000 on the controller GDT because of lack of collaboration. The Commissioner considered the position of the GDT to be in contravention of articles 30, 32 of the Law on Personal Data Protection, as well as article 77 of the Administrative Procedure Code because their responses were incomplete and inaccurate.[169]

166 According to article 23 of the Administrative Procedure Code, if the final decision on an administrative proceeding depends on taking a preliminary decision, which is in the competence of another administrative body or the court, the body that has the competence to make the final decision suspends the relevant proceeding until the other administrative body or the court have taken a preliminary decision. Exemption from this rule is allowed only in cases when failure to make an immediate decision causes irreparable damage to the fundamental constitutional rights of the parties.

167 With the exception of the case when otherwise envisaged in specific laws or imposed by special circumstances. In the case of special situations, the administrative proceeding concludes 3 months after the special situation has ended.

168 Regarding administrative investigations in the context of citizens' complaints, those that have targeted controllers in investigations by initiative have been merged into them, while the investigation into the political party Democratic Conviction lasted for almost one month.

169 Decision no. 41, dated 23.08.2021 of the CRIPDP
According to the letter of response to the Commissioner, the decision on the controller GDT was opposed at the Administrative Court of First Instance by the controller. The Court decided to send back the appeal without any action for procedural reasons. Therefore, the GDT has appealed it to the Administrative Court of Appeals in Tirana. The case is ongoing.

For all the investigated subjects, the Commissioner found it impossible to prove that the database was populated with data administered by these controllers.

The Commissioner concludes that in spite of legal-procedural steps to discover the source and creator of the database, the Office of the Commissioner did not find as proven any of the complaints to the relevant controllers, because referring to Part 1 of this Report, it was impossible to verify the connection of the controllers in question and the database. An exception is the media subject Lapsi.al, for which the CRIPDP was not able to conduct investigative actions, in the field or by official correspondence.[170]

The recommendations that have been issued to the subjects at the conclusion of the administrative proceedings on the voters' database indicate that:

- they are of a general nature,
- they do not envisage deadlines for fulfillment
- would be appropriate in the context of a thematic inspection and not in a case like this where the priority was to identify responsibilities for the breach of personal and sensitive data or their unauthorized processing by the relevant electoral subject.

The issued recommendations cover several directions and consist in aspects related to the security and confidentiality of data regarding adequate policies and procedures in managing activities of Information and Communication Technology, the establishment and management of ISMSs, etc.

2. The criminal investigation of the special prosecution office and the ordinary jurisdiction prosecution office

2.1 Denunciations

Based on article 283, paragraph 1, of the Criminal Procedure Code, every person who has become aware of a criminal offense that is prosecuted by initiative should file a referral on it.

a) Database of 910,000 voters

The electoral subject "Democratic Party" filed a criminal referral with the Special Prosecution against Corruption and Organized Crime against some state functionaries regarding the criminal offenses envisaged by article 328 "Active corruption in elections"[171] and article 122 "Spread of personal secrets,"[172] of the Criminal Code. The criminal referral was registered by this prosecution office on 14.04.2021 no.

170 See page 50 of the report

171 According to this provision, providing or giving money, material goods, promises of jobs or other favors in any form, for the voter or other persons related to him/her, for the purpose of taking a signature to present a candidate in elections, to vote a certain way, to participate or not in voting, or to engage in illegal activity to support a candidate or political party, is a criminal offense and punishable by imprisonment for one up to five years.

172 The dissemination of a secret belonging to the private life of a person by the person securing it due to their duty or profession, when forced to not spread it without being authorized, represents a criminal offense and is punishable by a fine or imprisonment for up to one year. this offense, committed for profit or to harm another person, is a criminal offense and is punishable by a fine or imprisonment for up to two years.

100, without any name (or suspected perpetrator) registered.[173] The subject of the referral is the publication of the database with personal data on the verge of the April 25, 2021, elections, namely 910,000 voters of Tirana, which showed the phone number, identification card number, voting center number, place of work, and a description of political affiliation.

b) Database of salaries and vehicles

Regarding the database of salaries and vehicles, based on official information made available to the AHC, it results that there have been no criminal referrals by citizens or other subjects.

2.2 Ex-officio investigation (by initiative of the prosecution office)

Based on articles 281, 282 and 283 of the Criminal Procedure Code, the prosecutor who becomes aware of the commission of a criminal offense or upon their own initiative, or from public officials, or medical personnel, or citizens.

a) Voters' database

Based on information obtained from the media, the Special Prosecution Office registered ex-officio the criminal proceedings no. 95 on 13.04.2021 about the massive breach of personal and sensitive data of Albanian citizens for the voters' database, regarding the criminal offense envisaged by article 122 of the Criminal Code "Dissemination of Personal Secrets" without any registered name (suspected perpetrator).

b) Salaries' database

Based on information offered in a response to AHC from the ordinary jurisdiction prosecution office of the Tirana judicial district,[174] the latter registered on its own initiative the criminal proceeding no. 9428 on 12.12.2021 for the criminal offenses of "Interference with computer data," "Interference in computer systems" and "Abuse of office," envisaged by articles 293/b[175], 293/c[176] and 248[177] of the Criminal Code. The target of the investigation has to do with the salary database circulated on social networks on 22.12.2021, which features the salaries of January 2021 of employees in state institutions and the

173 Referring to letter no. 2990/1 Prot. dated 15.04.2022 "Letter of Response" of the Special Prosecution Office against Corruption and Organized Crime to the Albanian Helsinki Committee

174 Letter no. prot. 5471/1 Prot/ S.M dated 14.04.2022

175 Damage, distortion, alteration, deletion, or unauthorized closing of computer data is punishable by imprisonment for six months up to three years. When this offense is committed in military computer data, of national security, public order, civil defense, health, or any other computer data of public significance is punishable by imprisonment of three up to ten years.

176 Creation of serious and unauthorized obstacles to harm the functioning of a computer system, through the insertion, damage, distortion, alteration, deletion, or omission of data, is punishable by three to seven years of imprisonment. When this offense is committed in military, national security, public order, civil defense, health computer systems or in any other computer system of national significance, it is punishable by five up to fifteen years of imprisonment.

177 Carrying out or intentionally not carrying out actions or inaction in violation of the law represents failure to regularly fulfill duties, by the person exercising public functions, when it has caused that person or others unjust material or non-material benefits or have harmed the legitimate interests of the state, citizens, and other legal entities, unless it represents another criminal offense, is punishable by imprisonment for up to seven years.

private sector. The data has been disseminated initially through the WhatsApp application and then were published in the media, thus becoming accessible by every citizen.

2.3 Decision making of the prosecution office for the start or non-start of the investigations

The criminal investigation starts officially the moment when the case is registered in the relevant prosecution office. Based on article 291 of the Criminal Procedure Code, upon registration of the criminal referral, the prosecutor has 15 days to decide on whether to start criminal proceedings.

a) Voters' database

Referring to the information obtained from the Special Prosecution Office,[178] after registering on its initiative the criminal proceeding no. 95, dated 13.04.2021 and the referral by the electoral subject "DP" no. 100 on 14.04.2021, it merged the two into one, no. 51, dated 14.04.2021. After merging the proceedings, this prosecution office began the investigation on the criminal offense "Active corruption in elections," envisaged by article 328 of the Electoral Code.

The prosecution office at the Tirana Judicial District Court also began to investigate this case, which was transferred to it by the Special Prosecution Office after five months of investigations.[179] On 26.10.2021, criminal proceeding no. 7681 was registered on the criminal offense "Unauthorized computer entry," envisaged by article 192/b[180] of the Criminal Code, without a registered name (or suspect).

b) Salary database

With the registration of criminal proceeding no. 9428 on 22.12.2021, the Tirana Judicial District Prosecution Office began investigations on its own initiative for the commission of the criminal offense "Abuse of office," committed in collaboration with others, envisaged by articles 248 and 25 of the Criminal Code, and the criminal offense "Passive corruption in the private sector," envisaged by article 164/b[181] of the Criminal Code.[182]

178 By means of letter no. prot. 1990/1 dated 15.04.2022,

179 By information offered by official letter no. 6708/1 Prot/ M.XH dated 11.05.2022 "Letter of response",

180 Unauthorized entry or entry that surpasses authorization to enter a computer system or part of it, through the violation of security measures, is punishable by a fine or imprisonment for up to three years. When this offense is committed on military, national security, public order, civil defense, health computer systems or oany other computer system of public significance, it is punishable by three up to ten years of imprisonment.

181 Seeking, obtaining, directly or indirectly, any kind of irregular benefit or promise of that, for oneself or others, or acceptance of an offer or promise, coming from irregular profit, by the person exercising a leadership function or working in any position in the private sector, to carry out or not carry out an action, in contravention of his/her duty/function, is punishable by imprisonment for six months up to five years.

182 Letter no. 5471/1 Prot/ S.M dated 14.04.2022 "Letter of response" by the Prosecution Office at the Tirana Judicial District Court to AHC.

2.4 Defendants

a) Voters' database

Criminal proceedings registered on the voters' database in the Special Prosecution Office, based on information provided officially, did not have registered persons as defendants.

b) Salary database

Based on information made available by the Tirana Judicial District Prosecution Office on the investigation of the salary database, it results that there were 4 citizens who were indicted as defendants, two of which employees in the public sector (NAIS) and two others in the private sector (company) as follows:

- E.Q, IT specialist at NAIS,
- A.A, IT specialist at NAIS,
- K.S, manager at company "Smart Collection" and
- E.I, general director in the company "Credit 2 ALL".

These citizens were charged with "Abuse of office" in collaboration with others and "Passive corruption in the private sector." Upon request of the prosecution office, the defendants were investigated while under security measure imposed by the Tirana Court.

2.5 Length of the criminal investigations

The Criminal Procedure Code envisages in article 323 that the deadline for concluding investigations is three months from the date when the name of the person whom the criminal offense is attributed to is noted in the register of announcement of criminal offenses, and six months for criminal offenses envisaged by letters "a" and "b" of article 75/a of this Code.

Article 234 of this Code, paragraphs 1 and 2, envisage that the prosecutor may extend the investigations for a period of up to three months. in the case of the Special Prosecution Office, this is up to six months. Further extensions, each for no longer than three months, may be made by the prosecutor in case of complex investigations or the objective inability to conclude them within the extended period. The length of preliminary investigations may not go beyond two years. Beyond the two-year deadline, for cases of charges for organized crime and crimes adjudicated by a panel of judges, the deadline may be extended only by approval of the General Prosecutor of the Chair of the Special Prosecution Office for up to one year, for each extension no more than three months, without infringing upon the deadlines for the length of pre-trial detention.

a) Voters' database

The Special Prosecution Office investigated on the criminal offense "Active corruption in elections" envisaged by article 328 of the Criminal Procedure Code, which refers to the case of the canvassers' database for a

5-month period.[183] On 30.09.2021, this prosecution office terminated investigations and declared lack of competence, transferring the investigation of this case to the Tirana Judicial District Prosecution Office.[184] The Tirana Judicial District Prosecution Office, in its information sent until the end of April 2022 said that the investigations were ongoing.

Although it has been more than one year from the start, not only is the criminal investigation not concluded, but there is nobody taken as a defendant in relation to this unprecedented incident in the country.

b) Salary database

On 09.05.2022, a release on the official website of the Tirana Judicial District Prosecution Office[185] communicated the conclusion of investigations started on 22.12.2021, regarding the publication of employees' salaries. As it results from the start and conclusion date for the investigations, this criminal investigation lasted for 5 months.

The investigation was conducted within a relatively reasonable timeframe, taking into account the complexity of the case, and was concluded fast compared to the criminal investigation on the voters' database, although the latter was registered eighteen months earlier.

2.6 Efficacy of criminal investigations

a) Voters' database

Based on information made available through official correspondence, the Special Prosecution Office initially conducted criminal investigations regarding the voters' database. This is the only information provided on the investigation by this prosecution office.

It is worth underscoring that although the Special Prosecution Office was asked for copies of decision making on the start of the criminal investigation and its cessation on the voters' database and the progress of further investigation of the cases by the Tirana Judicial District Prosecution Office, such information was not made available. AHC set into motion the CRIPDP, but in spite of the latter's request to the two prosecution offices, the information and documentation again was not made available.

In its response, the Special Prosecution Office referred us for more information to the Tirana First Instance Court Prosecution Office but did not respond to raised issues that are within its material competence. A special focus of the request for information was whether the Special Prosecution Office investigated high-level functionaries of the institutions from where it is suspected the data breaches occurred (NAIS, Ministry of Economy and Finance), how collaboration was between prosecution offices and other law enforcement and public bodies was on the investigations, whether there were difficulties in obtaining and collecting evidence, etc.

183 From the date the criminal referral was registered (14.04.2021) until the daty when lack of competence was cited, a period of 5 months went by.

184 Letter no. 2990/3 Prot dated 10.05.2022 "Letter of response," Special Prosecution Office against Corruption and Organized Crime.

185 https://www.pp.gov.al/Tirane/Media/Prokuroria_prane_Gjykates_se_Shkalles_se_Pare_Tirane_perfundon_hetimet_per_procedimin_penal_nr_9428_te_vitit_2021_me_objekt_hetimi_publikimin_ne_rrjetet_sociale_ne_date_22_12_2021_nepermjet_aplikacionit_WhatsApp_te_listes_se_pagave_Janar_2021

As it underscored in the annual human rights report for 2021,[186] AHC considers that the investigation of the Special Prosecution Office, in keeping with the material competence and circle of subjects, should have extended also to the senior public officials of state institutions, due to the responsibilities that these institutions have for guaranteeing the security and protection of data they are in contact with and from where the breach may have come. This information of high public interest, although the criminal case has been terminated by the Special Prosecution Office, has not been made public and it has been avoided in the document in response to AHC.

Regarding the progress of the investigation into this case by the Tirana Judicial District Prosecution Office, after SPAK declared its lack of competence, it is noted that information is missing also, on grounds that it is a secret of the investigation.

b) Salary database

Based on the official announcement on the conclusion of criminal investigations into this case, the Tirana Judicial District Prosecution Office conducted investigations on 2 NAIS employees for charges of "Abuse of office," "Passive corruption of individuals exercising public functions" and for the two other defendants, employees in the private sector, on the criminal offense of "Active corruption of individuals exercising public functions."

Procedural actions to investigate the salary database were conducted dynamically and within short deadlines as the prosecution office issued three orders on 23.12.2021, one day after the publication of the news, ordering the holder (administrator) or controller of computer data of the NAIS, GDT, and the Tirana Social Insurance Institute to hand over computer data memorized in the computer system, concretely of all logs into the data system for the salaries of January 2021. The orders were executed by the judicial police with the relevant process-verbals of 23.12.2021.

Based on investigative acts, according to the process-verbal of the review of the work e-mail of IT specialist at the GDT, with the initials E.Q., it was found that the requested and published data that were the subject of the investigation had been sent from her work e-mail, to the work e-mail of the citizen with initials A.A., a specialist at NAIS. Concretely, the data was sent in 6 communications spanning over the period of one year, during the period October 2020 – October 2021, as follows:

- The list of payments for September 2020 was sent on 21.10.2020.
- The list of payments for October 2020 was sent on 25.11.2020.
- The list of payments for December 2020 was sent on 25.01.2021.
- The list of payments for January 2021 was sent on 24.02.2021.
- The list of payments for March 2021 was sent on 29.04.2021.
- The list of payments for September 2021 was sent on 22.10.2021.

This information appears to have been sent form the work address of the NAIS specialist to the electronic address of her colleague, another employee at NAIS, with initials A.A. These electronic data files, based on the review, were sent through the program We Transfer.

186 Raporti-Vjetor-per-te-Drejtat-dhe-Lirite-e-Njeriut_2021_KShH-_Final.pdf (ahc.org.al)

In the context of this criminal proceeding, the Tirana Judicial District Prosecution Office sought to review the conduct of expertise of the sequestered computers possessed by the two NAIS specialists (E.Q. and A.A.) as well as the hard disk sequestered from citizen K.S.

Based on the experts' reports ordered by the prosecution office,[187] it results that in all three computers there were found and recuperated some document files in the "Excel" format, titled "21.10.PaymentListTotal.xlsx' and 'Salaries January 2021.xlsx.' These files contained the requested data in the decision of experts where salaries of different citizens were found in the "excel" format alongside columns named as follows:

- Personal number,
- Name, family name,
- Period,
- Is Albanian,
- Business Registration Number,
- Subject,
- Category and type of business.
- RetunDate,
- DRT,
- Daysworked,
- Gross salary,
- Salary, contributions, social contribution, employer's contribution, employee's contribution, supplementary contribution, health contributions,
- Personal Income Tax,
- Profession.

Regarding their contents, although these files contain differences regarding the formatting of the listing of names and number of columns, after comparison and testing of some names, there is full match of data in different columns.

In reference to this fact resulting from the criminal investigation, it is worth mentioning that this comparison and testing of some names could have been conducted (but effectively was not) even during the inspection conducted by the Commissioner, in the context of the administrative investigation on the first database of voters. Therefore, in the context of these investigations, joint coordination of work, without infringing upon the competences of each institution, would be essential.

Also, in the hard disk that was reviewed by experts,[188] belonging to citizen K.S., aside from documents containing the words in the review decision, there was a considerable number of other documents with bank data about different clients.[189] It is unclear how such data was obtained and whether the prosecution office referred them for administrative investigation of subjects (controllers in the banking sector or beyond) that are in contact with such data.

187 No. 259 Prot, no. 256 Prot and no. 255 Prot dated 22.02.2022.
188 Experts' report no. 259. Prot dated 22.02.2022.
189 https://shqiptarja.com//uploads/ckeditor/62840c6b88a45CamScanner%2005-16-2022%2023.14%20(1)_001.pdf

2.7 Decision making of the Prosecution Office

Until May 9, 2022, the Tirana Judicial District Prosecution Office, at the conclusion of its investigations,[190] submitted the request to send the case to court against the four defendants:

1.7.1 E.Q., accused of committing the criminal offense "Abuse of office," committed in collaboration with others, envisaged by article 248 and 25 of the Criminal Code.

1.7.2 A.A., accused of committing the criminal offense of "Abuse of office, committed in collaboration with others," envisaged by articles 248 and 25 of the Criminal Code, "Passive corruption of individuals exercising public functions," envisaged by article 259 of the Criminal Code.

1.7.3 K.S., accused of committing the criminal offense of "Active corruption of individuals exercising public functions," "Passive corruption in the private sector," envisaged by articles 244 and 164/b of the Criminal Code.

1.7.4 E.I., accused of committing the criminal offenses of "Active corruption of individuals exercising public functions" and "Passive corruption in the private sector," envisaged by articles 244 and 164/b of the Criminal Code.

Referring to article 75/a, letter "a"[191] and article 80, paragraph 1[192] of the Criminal Procedure Code, it is notable that that two of these criminal offenses are the material competence of the Special Court against Corruption and Organized Crime. As a result, for their investigation, the material competence belongs to the Special Prosecution Office[193] and not the Tirana Judicial District Prosecution Office. These two criminal charges are investigated and adjudicated by the specialized institutions in the fight against corruption and organized crime, as they have to do with "Passive corruption of individuals exercising public functions"[194] and "Active corruption of individuals exercising public functions."[195] It is unclear in what conditions and circumstances, and therefore what legal basis, these citizens were investigated by the Tirana Judicial District Prosecution Office for criminal offenses that are the material competence of SPAK and the SCCOC.

190 https://shqiptarja.com//uploads/ckeditor/62840c6b88a45CamScanner%2005-16-2022%2023.14%20(1)_001.pdf

191 Special Court against Corruption and Organized Crime adjudicates: a) crimes envisaged by articles 244, 244/a, 245, 245/1, 257, 258, 259, 259/a, 260, 312, 319, 319/a, 319/b, 319/c, 319/ç, 319/d, 319/dh and 319/e; … …

192 In cases of proceedings linked between them and that may not be separated, of which one or some are the competence of the Special Court against Corruption and Organized Crime and other proceedings are the competence of other first instance courts, the Court against Corruption and Organized Crime shall be competent.. … …

193 Article 8 of law no. 95/2016 "On the organization and functioning of institutions for fighting corruption and organized crime" envisages that the primary material competence of the SCCOCs is envisaged in article 75/a of the Criminal Procedure Code, but may not surpass the competence stipulated by article 135, paragraph 2, of the Constitution; 2. The Court against Corruption and Organized Crime and the Special Prosecution Office are competent for reviewing, investigating, and prosecuting any criminal offense, according to paragraph 1 of this article, even in cases when no charges are brought against an official, according to article 135, paragraph 2 of the Constitution, or against a principla official of a central or independent institution, according to this law.

194 Envisaged by article 259 of the Criminal Code

195 Envisaged by article 244 of the Criminal Code

CHAPTER VI

Recommendations

In order to adapt the domestic regulatory framework to the standard of the Regulation, and to address some of the problems encountered by the continued massive data breaches, the following amendments to our legal framework are recommended:

1. A broader definition of personal data and envisioning the extra-territorial effect of the law (i.e., beyond the territory of the Republic of Albania) also for activities that harm the interests of individuals operating inside our territory.
2. Strengthening the existing rights of personal data subjects and expansion of rights according to the spirit of the Regulation, so that the subjects have more control over the administration of their personal data. Aside from consolidating existing rights, the package of the subjects' rights should be expanded also through recognition of the "right to be forgotten" and the possibility for data portability.
3. Expanding the obligations of controllers/processors through expansion of existing obligations and provisions of additional obligations. The latter should be more responsible toward personal data subjects and should have the obligation to prove the compliance of their activity with the requirements of the law.
4. Envisaging in the law the specialized structure tasked with respect of the compliance of the controller's activity with the requirements of the law. This role will be played by the Personal Data Officer (PDO) who will lead to increased attention by the controller to personal data protection. This new obligation for the controller will require staff that is trained on the law and the drafting of manuals to help PDOs.
5. Clearly defining the obligation of controllers to notify about massive data breaches, not only to the Commissioner, but also to the data subjects, should the breach impact their rights. This notification should be conducted immediately after the controller becomes aware of the breach of such data.
6. Strengthening the standing of the Commissioner, by consolidating his independence and by recognizing legally as duties of the Commissioner the increased public awareness and understanding of the risks, rules, guarantees, and rights regarding the processing, with special focus on activity toward children, increased awareness of controllers and processors on the obligations deriving from the law on personal data protection, overseeing developments that may impact personal data protection, encourage the drafting of codes of conduct, etc.
7. Adapting the needs of the Commissioner according to changes in the framework of his competences, securing an increase of human, technical, and financial capacities.
8. Amending the regime of fines by increasing their level and making it more effective, certainly maybe adapting it to the country's economic development.
9. Specifying legal means available to data subjects for the protection of their rights (complaining to the Commissioner and complaining directly to the court).
10. For the most complete protection of data subjects' rights and to facilitate their access to justice, especially in cases of massive data breaches, it is recommended that the law recognize the possibility to file representative action without an authorization by the damaged subjects. In this regard, the approval of the law "On representative action" will be helpful.
11. Pursuant to the practical implementation of provisions, the Commissioner should exercise more effective control of his recommendations for controllers by establishing significant sanctions in case of failure to respect the Commissioner's instructions.

12. Drafting instructions for the protection of data during electoral campaigns (per the Commission's Guidelines)[196] by defining clear tasks for each of the actors, starting with political parties, candidates, or the Central Election Commission that may be in the role of controllers as well as third parties that may be contracted by them and be as co-controllers or processors.
13. Harmonizing personal data protection with freedom of expression, by clearly defining in what cases one or the other prevails. Such balancing should be done by law and by respecting the essence of these fundamental rights, be proportional and necessary.
14. Updating other legal parts that are linked with personal data protection such as the "Law on Electronic Communications," which has not been fully updated per the Directive that is in force and requesting full implementation of these provisions.

196 On the Implementation of Union legislation for the Protection of Personal Data in the Electoral Context

BIBLIOGRAPHY

Legislation

- Constitution of the Republic of Albania, law no. 8417, dated 21.10.1998, amended.
- Criminal Code of the RA
- Criminal Procedure Code of the RA
- Administrative Procedure Code
- Law no. 9887, dated 10.3.2008 "On personal data protection," amended.
- Law no. 9288, dated 7.10.2004, On the Ratification of the Convention "On the Protection of Individuals in Relation to the Automatic Processing of Personal Data," amended
- Law no. 9918, dated 19.5.2008 "On electronic communications," amended, Law no. 10325, dated 23.9.2010, "On State Databases"
- CMD no. 1147, dated 9.12.2020 "On the creation of the state database 'Unique Government Portal E-Albania' and the approval of rules 'On the functioning of the Single Contact Point"

International Acts and EU Legislation

- European Charter of Fundamental Rights, 2012/C 326/02, published in OJ C 326, 26.10.2012.
- Convention for the Protection of Persons from Automatic Data Processing, Council of Europe, STCE no. 108, 1981. https://www.coe.int/en/web/conventions/full-list?module=treaty- detail&treatynum=108
- Protocol Amending the Convention for the Protection of Individuals from Automatic Processing of Personal Data, approved by the Committee of Ministers, May 18, 2018.
- Regulation (EU) 2016/679 (General Data Protection Regulation) published in OJ L 119, 04.05.2016.
- Regulation (EU) 2018/1725 of the European Parliament and the Council of October 23, 2018, on the Protection of Individuals with Regard to the Processing of Personal Data by Institutions of the Union, bodies, offices, agencies, and free movement of such data, which invalidates Regulation (EC) No 45/2001 and Decision no. 1247/2002/EC
- Regulation (EC) 45/2001 of the European Parliament and the Council of December 18, 2001, on the Protection of Individuals with Regard to the Processing of Personal Data by Community Institutions and Bodies, and the free movement of such data,
- Directive (EU) 2016/680 of the European Parliament and Council of April 27, 2016, on the protection of individuals from the processing of data by competent authorities for the purpose of preventing, investigating, discovering, or prosecuting criminal offenses or the execution of criminal sentences and on the free circulation of such data, invalidating the Framework Decision of het Council 2008/977/JHA.
- Directive 2002/58/EC of the European Parliament and Council of July 12, 2002 on the processing of personal data and the protection of privacy in the sector of electronic communications (Directive on privacy and electronic communications), amended.
- Instruction of the Commission on the Implementation of the Union Law on Data Protection in the Electoral Context.

Reports of the EU, international organizations, or internationally known

- file:///C:/Users/user/Downloads/Albania-Report-2021%20(6).pdf
- ALBANIA 2021 HUMAN RIGHTS REPORT (DOS)
- https://www.osce.org/files/f/documents/4/c/495052.pdf
- Amnesty International Report on Human Rights
- https://freedomhouse.org/country/albania/freedom-world/2022
- Communication of the Commission to the Parliament and the Council, Data protection as a pillar of empowering citizens and EU's Approach to the digital transition – two years of application of the General Data Protection Regulation, SWD(2020)115 final.
- Position and findings of the Council on the application for the implementation of the General Data Protection Regulation, Brussels, January 15, 2020, 14994/2/19
- Annual Report 2021, Commissioner on the Right to Information and Personal Data Protection,
- Commission Staff Working Document, SWD(2020) 354 final, Albania Report 2020, 6.10.2020.
- Commission Staff Working Document Report, Albania 2021, SWD (2021) 289 final 2021.
- European Data Protection Supervisor, Opinion 6/2015, An important step toward inclusive EU data protection, October 28, 2015

Doctrine

- S. Rodota, "Data Protection as fundamental Right", in S. Gutwirth et al, (Eds) Reinventing Data Protection?, Springer 2009.
- Th. Streinz, The Evolution of European Data Law, published in P. Craig and G. de Burca (eds), The Evolution of EU Law, Oxford university Press, 2021, f. 902-936
- Ch. Kuner, et al, The Eu General Data Protection Regulation: A Commentary, Oxford University Press, 2021
- T. Mulder, Health Apps, their Privacy Policies and the GDPR, European Journal of Law and Technology, Vol 10, no.1, 2019.
- Ch. J., Hoofnagle et al, The European Union General Data Protection Regulation: what it is and what it means, Information and Communications Technology Law, 2019, Vol 28, No.1, 65-98.
- E. Kosta, Peeking Into the Cookie Jar: the European Approach Towards the Regulation of Cookies, International Journal of Law and Information Technology (2013) 21(4)
- Douwe Korff and Marie Georges, The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, July 2019

Jurisprudence

- Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C-131/12 ECLI:EU:C:2014:317.
- Maximillian Schrems v Data Protection Commissioner C-362/14, ECLI: EU:C:2015:650.
- Comission v Hungary C-288/12 ECLI:EU:C:2014:237, 8 April 2014
- Meta Platforms Ireland Limited, formerly Facebook Ireland Limited v Bundesverband der Verbraucherzentralen

und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. C-319/20, ECLI:EU:C:2022:322.

- C-73/07, Tietosuojavaltuutettu kundër Satakunnan Markkinapörssi Oy dhe Satamedia Oy, 16 dhjetor 2008, para. 56, 61 and 62
- ECtHR-Satakunnan Markkinapörssi Oy and Satamedia Oy V. Finland, Nr. Aplikimi no. 931/13

Media sources

Ekskluzive/ Si na monitoron Rilindja nr e telefonit, nr ID, vendet e punës, të dhënat konfidenciale për 910 mijë votues të Tiranës – Lapsi.al

https://lapsi.al/2021/12/22/superskandali-dalin-sheshit-emer-per-emer-rrogat-e-mbi-600-mije-shqiptareve/

https://news-31.com/news/thellohet-sandali-publikohet-databaza-me-targat-e-makinave-i22293

https://lapsi.al/2021/04/11/alibia-e-taulant-balles-per-pergjimin-qe-ps-u-ben-te-dhenave-personale-te- qytetareve/

https://lapsi.al/2021/04/13/rama-pranon-patronazhistet-kemi-vite-qe-i-kemi-shperndare-ne-terren/

COURT-7003525-v2-20204_21_LE2_2a_R39_Granted_Only.pdf (reporter.al)

https://a2news.com/2022/01/07/skandali-i-publikimit-te-pagave-4-te-arrestuar-prokuroria-zbardh-skemen-do-ti-shkohet-deri-ne-fund-cdolloj-subjekti-te-perfshire/

https://shqiptarja.com//uploads/ckeditor/62840c6b88a45CamScanner%2005-16-2022%2023.14%20(1)_001.pdf