IMPACT OF IMPLEMENTING GDPR LEGISLATION ON EMPLOYMENT IN ALBANIA

Deloitte. Legal

OCTOBER 2019

PREPARED BY:
DELOITTE
LEGAL ALBANIA

Commissioned by:

RisiAlbania, a project of the Swiss Development Agency for Development and Cooperation (SDC) implemented by Helvetas Swiss Intercooperation and Partners Albania for Change and Development.

Disclaimer:

The report should not be regarded or relied upon as being a comprehensive or formal legal opinion concerning any matters referred in it. It has been prepared as a general summary of certain features of the legal framework, documentation and information reviewed by Deloitte and should not be treated as a substitute for specific legal advice concerning individual matters, situations or concerns. Deloitte does not bear any liability toward any third parties whosoever for any reliance whatsoever on the content of the Report. In addition, neither the Deloitte nor any of its partners, directors, officers, employees, representatives, advisers or agents shall be liable for any direct, indirect or consequential loss or damage suffered by any person as a result of reliance on any statement or on the basis of any omission in any information supplied with this Report or in any other written or oral information made available and any such liability is expressly disclaimed.

This version of the report has been modified.

CONTACT INFO@RISIALBANIA.AL TO REQUEST A FULL VERSION OF THE REPORT

PUBLISHED BY RISI ALBANIA
A PROJECT OF THE SWISS AGENCY FOR DEVELOPMENT AND COOPERATION (SDC), IMPLEMENTED BY HELVETAS AND PARTNERS ALBANIA

RisiAlbania
Partner for Growth

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Agency for Development and Cooperation SDC

REPUBLIC OF ALBANIA
PRIME MINISTER'S OFFICE
DEPUTY PRIME MINISTER

HELVETAS Swiss Intercooperation ALBANIA

PARTNERSALBANIA FOR CHANGE AND DEVELOPMENT

Abbreviations

ALL	Albanian Leke
ATS	Applicant Tracking System
Bln	Billion
BoA	Bank of Albania
BPO	Business Processes Outsourcing
c.	Circa
Commissioner	Commissioner for Freedom of Information and Personal Data Protection
Deloitte	Deloitte Legal Shpk and Deloitte Albania Shpk
DPO	Data Protection Officer
EU	European Union
EU Commission	European Commission
EUR	Euro
GDPR	REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
ICT	Information and Communication Technology
Mln	Million
SME	Small and medium-seized enterprises
TELCO	Telecommunication industry
Thsd	Thousand

Table of Contents

1. INTRODUCTION 5

1. 1. The Report 5

1. 2. Scope and limitations of the report 6

1. 3. Key highlights 7

2. STRUCTURE AND METHODOLOGY 10

2. 1. Structure of the report 10

2. 2. Methodology 11

3. REPORT 13

3. 1. Potential impact from GDPR enforcement in the Albanian business environment 13

3. 1. 1. GDPR 13

3.1.2.1 Rights of data subject 16

I. Right of information 17

II. Other rights 18

3.1.2.2 Data controller and data processor 20

3.1.2.3 Personal data security 22

3.1.2.4 Data Protection Officer 25

3.1.2.5 International transfer of personal data 26

I. Transfer based on an adequacy decision 26

II. Transfer subject to appropriate safeguards 26

III. Transfer based on derogations for specific situations 27

3. 2. PART # 2 –The economic sectors that will be affected by the implementation of GDPR 29

3. 2. 1. Legal perspective 29

3.2.1.1 Processing of personal data in education sector 30

3.2.1.2 Processing of personal data in healthcare sector 30

3.2.1.3 Processing of personal data in journalistic sector 31

3.2.1.4 Processing of personal data in banking sector 31

3.2.1.5 Processing of personal data in sector of hotel services 32

3.2.1.6 Processing of personal data in telecommunication sector 32

3.2.1.7 Processing of personal data for direct marketing 33

3.2.1.8 Processing of personal data for employment purposes in private sector 33

3.2.1.9 GDPR's sectoral related provisions 34
3. 2. 2. Case studies: potential effects of the GDPR on several Sectors 34
I. Information and Communication Technologies (ICT) Sector 35
II. Financial sector 37
III. Business Process Outsourcing industry 38
IV. Healthcare sector 39
3. 2. 3. ICT and information security 40
3. 2. 4. GDPR impact from technology and information security perspective 41
3. 3. Job creation stimulation by GDPR implementation in specific economic sectors 42
3. 3. 1. Impact assessment 42
3. 3. 2. Industry-based analysis 43
BPO Sector 43
BPO – ICT profile 44
Banking sector 45
Telecommunication sector 46
3. 3. 3. Conclusions 47
3. 4. Estimation of the period of implementation of GDPR legislation in practice 49
3. 4. 1. Approximation instrument and procedure 50
3. 4. 2. Proposed transitory period 51
3. 5. How GDPR compliance could stimulate development of business consultancy services 53
Assistance from business consultancy services in the initial implementation phase 53
GDPR impact on Albanian ICT and information security consultancy services 53
3. 6. Assessment of how GDPR can lead to new investments and increased competitiveness 54
GDPR impact on local investment 54
GDPR impact on foreign investment 55

1. INTRODUCTION

1. 1. The Report

Privacy is no longer just a legal, compliance or security issue; it has become a strategic topic at the boardroom level and even more so since approval of GDPR. The GDPR, which came into effect on May 25, 2018, has repealed the Directive 95/46/EC. A core feature of the GDPR is that as a regulation, rather than a directive, it does not require to be implemented through a national law in each EU Member State, by shrinking the discretional room of the latter significantly. The harmonization of personal data protection through GDPR is expected to reduce local complexities and duplicative administrative burdens such as registrations.

Albania is expected to open its accession negotiations with EU on October 2019. As stipulated in paragraph 3 of article 70 of the SAA[1], data protection is one of the fundamental elements of the EU *acquis*, for which Albania has undertaken the commitment of approximation of its legislation on the first stage of SAA, making the adoption of GDPR to Albanian data protection legislation a priority.

The protection of personal data represents a constitutional imperative, laid down under article 35 of the Constitution of the Republic of Albania. Except for that, other important instruments dealing with the same subject matter are the international treaties transposed into national legislation, the Law on Personal Data Protection and the sublegal acts issued based thereon. The Law on Personal Data Protection is fully aligned with Directive 95/46/EC. In addition, since its approval, the Commissioner has issued more than 55 sublegal acts (i.e. decisions and instructions) in application to such law, which, on the other hand, represent the continuous attention and attempt of this authority to keep up the pace of the most important developments of personal data protection legislation in the EU.

Arguably, GDPR has brought novelties, in terms of rights of information to be provided to data subjects, rights of the latter and, subsequently, obligations of data controllers. In addition, it has significantly increased the administrative fines that would be imposed in case of breaches of applicable legislation (including, but not limited to, data breaches).

The objective of the Report is to evaluate how the enforcement of GDPR would impact the business environment in Albania and the Albanian economy.

[1] Article 70, Paragraph 3 of the SAA: "During the first stage of the SAA as defined in Article 6, approximation shall focus on fundamental elements of the internal market acquis as well as on other important areas such as competition, intellectual, industrial and commercial property rights, public procurement, standards and certification, financial services, land and maritime transport — with special emphasis on safety and environmental standards as well as social aspects — company law, accounting, consumer protection, data protection, health and safety at work and equal opportunities. During the second stage, Albania shall focus on the remaining parts of the acquis".

1. 2. Scope and limitations of the report

The scope of this Report is to provide high-level conclusions on the types and potential impact from enforcement of GDPR in the Albanian legislation and business environment.

On the focus of the scope of the Report will be the identification of economic sectors that would be affected, the assessment whether and how the implementation of GDPR would stimulate job creation and sectoral employment potential, business consultancy services, as well as the potential new investments and competitiveness of economic sectors.

Moreover, it aims to provide a mere estimation of the implementation of GDPR legislation in practice.

Despite the above, the scope of this Report is subject to the following limitations and qualifications:

The Report provides a description and comparison of the legal requirements on personal data protection in force in Albania, with the provision of GDPR, as well as a 'snapshot' of personal data protection situation from the view of the interviewed organizations. As such, the analysis is based on the material aspects that, to our understanding, would be introduced into Albanian legislation in the ambit of alignment with GDPR. Hence, in any case, the conclusions of this Report are not to be viewed as exhaustive. They, rather, represent a general assessment of how the future of personal data protection (in different sectors) might (not 'will') be or look like following the implementation of GDPR.

The Report makes use of some external information prepared by different private and public research organizations. As the information used has been collected from multiple sources, sets of data may not be totally consistent with one another.

Additionally, there may be inconsistences between data gathered from various public sources and data gathered from interviews. Data from public source are on a macro-level, while data gathered during interviews are focused on specific pool of companies in each sector, targeting specific companies.

Our procedures and enquiries do not constitute a review of the accurateness or completeness of information provided to us or the information collected from public sources.

More, information used in the analysis includes unaudited information and may not have been corroborated. Accordingly, we accept no responsibility for the reliability of the information to the extent it is inaccurate, incomplete or misleading, or for matters not covered by the Report or omitted due to the limited nature of our work.

Our overlook of the economic impact is based only on ex-ante analysis of the GDPR impact in Europe, no post-implementation analysis is undertaken. Therefore, there is a lack of qualitative and quantitative data comparison, thus the walkthrough of the economic impact of GDPR in Albanian is limited.

Our work is based, also, on the following:

- Desk review of legal and regulatory framework and other labor market relevant data to define skills, capabilities and expertise required, as well as job positioning in organizational setup for GDPR implementation;
- Review of all available data, policies and strategies about BPO industry development opportunities in Albanian market;
- Qualitative interviews with representatives of entities operating currently in BPO industry in the Albanian market.

During the interviewing phase, we have faced some obstacles in obtaining information from some of the companies, targeted for direct interviews. The hesitation was mainly caused due to a low awareness of these companies on GDPR, confidentiality reasons and in some cases, due to the unavailability of the companies' representatives to provide us with the required information. Moreover, during our desk review, we have faced some obstacles in data research since there are limited formal and public sources of updated data available for the BPO industry.

1. 3. Key highlights

The Report provides an analysis of the impact of GDPR implementation in the Albanian economy, particularly in some of the industries that process a high volume of personal data such as information and communication technologies (ICT), financial industry, business process operation (BPO) and healthcare.

- The service sector, including data controllers and processer companies, is expected to be one of the main contributors in country's GDP and employment. The young, low cost and highly technology friendly labor force, as well as the favorable fiscal policies are expected to drive the growth of this sector.
- For the industries under analysis, mentioned above, it is expected a short-term increase in expenditures in order to be GDPR compliant. However, in the long term, this regulation is forecast to bring economic benefits due to the increase of customer confidence in compliant companies, the improved data managing and processing of information, as well as the increased potential for business opportunities from EU countries.
- Based on a study conducted by London Economics it was estimated the potential effect of GDPR in UK. Therefore, throughout this study, based on triangular methodology, we have estimated the potential impact in the Albanian economy. In Albania, the overall spending for third party data will decrease by approximately 10.5% but the costs will not follow the same decreasing trend. Sectors related to marketing and advertising are estimated to have a decrease in profit of approximately 340 thousand Euro p.a. However, the implementation of GDPR will

make third party data more valuable thus being beneficial to the providers of data.

- According to a study from Netapp, overall for countries which have a strong local regulation the ICT sector as a whole is not expected to shrink as such companies can be considered partially prepared to implement the regulation. The impact on companies, which are part of international franchises, is expected to be similar to the one of their parent companies.

As per a study prepared from Deloitte UK on the Potential Impact of the Proposed Regulation, Direct marketing, Web analytics and Credit Information impact from GDPR is expected to be largely offset by new outsourcing opportunities from EU countries. However, we estimated that the impact of this sector in GDP at the worst-case scenario would cause a decrease on the range between 0.5% and 0.6%, mainly due to initial implementation costs.

In addition to the above, the report provides the reader with a general overview on the level of awareness, knowledge and expertise of the Albanian companies on GDPR legislation and an industry-based analysis focusing on: BPO, BPO with an ICT focus, Telecommunication, Banking and Healthcare Tourism. The scope of the analysis is to draw insights on the perception of such businesses on the impact of the GDPR implementation in the Albanian economy and employment growth.

Albanian companies are knowledgeable and claim to posses expertize on the Albanian legislation on personal data protection. However, most of them appear to be unsure of how to approach the GDPR. They have adopted a “wait and see” approach and expect further instructions from the Commissioner before taking any action towards GDPR implementation.

The interviewed businesses expressed that in their view, the harmonization of the Albanian legislation with GDPR, will create new opportunities for services and business expansion for the BPO sector. On the other hand, the majority of BPO companies claimed that the implementation of the GDPR requirements would at least enable them to retain the current business and potentially expand further the range of services provided for EU market. The interviewed companies that claim to have implemented GDPR standards as imposed by their EU or non-EU based holding companies admit to have gained as a result, a competitive advantage in the market.

The increasing trend of the BPOs, in terms of economy and employment in Albania, (section 3.3.1), together with the analysis of the structured interviews conducted with the businesses, indicates that the GDPR adoption into the Albanian legislation might be put higher in the list of priorities in the approximation of legislation with *Acquis Communautaire*. This would provide the BPOs the likelihood for further growth in Albania, by leveraging on the competitive advantage in terms of labor costs, geographic position, and skills, to exploit the full unexplored business

potential with EU based contractors. This would be a benefit for the BPO industry and would be an opportunity for the Albanian market economy and employment growth.

On the opposite side of the spectrum, the BPOs falling into the category of small size enterprises, might find it difficult to cope with the adoption of the GDPR. This is expected to be a result of being relatively financially weak to fund the technological changes, especially taking into consideration of having no parent company to support them in terms of expertise and investment.

All BPOs would need to start their journey toward GDPR implementation by taking the necessary steps starting with an assessment process, which would help them identify gaps and allocate budget for new technologies, staff upskilling and related consulting services.

In terms of what will be the expertise needed for GDPR implementation, there is a great potential and new opportunities for the consulting business, specialized in personal data protection and GDPR requirements implementation and more specifically in IT and Legal expertise.

Based on structured interviews' results, most companies plan to hire external consulting firms to support them with the preparations for the implementation and post-implementation of the GDPR requirements. The GDPR's requirements are deep and complex. Preparation for its implementation requires buy-in and support from across the organization. Companies have come to an understanding that they do not posses the right expertise to handle the implementation on their own.

Based on findings from the structured interviews, BPO companies with an ICT focus estimate that in case of GDPR adoption into Albanian legislation, they expect a potential growth in terms of business and employment in their area of expertise. They believe the company reputation will improve as GDPR compliant ones, improving at the same time their competitive advantage in offering services and doing business with EU based contractors. Therefore this expected expansion would create more job opportunities of in a vast range of job profiles in services these BPOs are actually operating as ICT, Call Operators, Tourist agents (call centers,) Finance and Accounting, Technical Support Specialists, Loan & Card Collection agents (please refer to Table 1, page 80 of this report).

Concerning specifically the ICT sector, GDPR requirements would mainly have an impact on the following areas:

- *ICT consultancy providers* that offer expertise in privacy data protection across organizations and GDPR related services are expected to have a demand in areas such as: GDPR readiness assessment / Gap Analysis, Internal Audit, Cybersecurity, IT training and awareness, GDPR implementation and Continual Maintenance, etc.
- *Enforcement of Cybersecurity policy and practice* would result in reduction of attacks and data breaches, as well as better

understanding of what is going on across the network.

Technological improvement coming from GDPR adoption would result in competitive advantage for Companies in several directions such as: Better Decision Making and Better Personalized Services for Customers; Innovation within Company; Reduced IT Maintenance Costs by the retiring of data software and/or applications that are not relevant or compliant.

2. STRUCTURE AND METHODOLOGY

2. 1. Structure of the report

The report is divided into three chapters: Introduction (*chapter 1*), Structure and Methodology (*chapter 2*) and Report itself (*chapter 3*).

Chapter 3, being the most important one, is further broken down into six subchapters (i.e. parts), from 3.1 to 3.6, which convey our understanding and approach from the legal, economic, ICT and employment related perspective the impact of GDPR following its implementation in the Albanian legislation.

Subchapter 3.1 (Part # 1) provides a comparative analysis of the main differences between Albanian and GDPR legal provisions, with summarized information that emphasizes the areas of the national legislation aligned with GDPR provisions.

Subchapter 3.2 (Part # 2) assesses the sectoral impact of the implementation of GDPR legislation, from the legal, economic and, specifically, ICT perspective. The legal assessment relies on the sublegal acts of the Commissioner dealing with processing of personal data in different sectors. From the economic perspective, the sectoral impact of GDPR will be assessed through a high-level cost-benefit analysis. A special focus is awarded to the impact of GDPR implementation on ICT sector, by indicating the main requirements of such instrument that might lead an organization to require technology innovation.

Subchapter 3.3 (Part # 3) contains a general description and overview of the BPO industry in Albania, and a section dedicated to analysis and high-level assessment of BPO industry development and its growing importance in the Albanian economy, based on data gathered from available public sources. Finally, the reader might consult the relevant conclusions based on the overall assessment conducted.

Subchapter 3.4 (Part # 4) contains a general analysis and specific conclusions on the sort of legal instrument that might be used for purpose of aligning the Albanian legislation with the provisions of GDPR. Moreover, its conducts an evaluation of the transitional period that would be reasonably needed for an organization to be able to adapt to the introduced novelties of GDPR (i.e. following its implementation).

Subchapter 3.5 (Part # 5) evaluates how GDPR compliance would stimulate the development of consultancy services in Albania (i.e. especially the

impact and effects on the ICT consultancy services). It includes business consultancy development in Albanian market as a result of GDPR enforcement. As already known, the road to GDPR compliance might be complex and many organizations would need help from experienced third parties.

Subchapter 3.6 (Part # 6) introduces to the readers the potential for new local and/or foreign investments as result of GDPR compliance. This analysis is based on best practices of countries in the region or above. In conclusion, it contains a walkthrough in regard to the expected effects of GDPR implementation in terms of attracting new local and foreign investments in Albania.

2. 2. Methodology

In order to obtain a clear view on GDPR impact in Albanian businesses and to further assess the potential impact of implementation of GDPR on the Albanian market we have used the approach described below:

- Legal review and comparison of the current Albanian legal framework on personal data protection and provisions of GDPR.
- Benchmark analysis of the GDPR impact in Albania and in other countries, which have already adopted the GDPR. Overlook of the economic impact on several sectors in Albania, as a reference with other countries.
- Desk review and research to create a general market overview and understanding. We have gathered and analyzed data from different sources such as public and governmental institutions with regard to BPO industry in Albania. This was associated with research and analysis of labor market for BPO industry with the focus on it potential for further growth especially with regard to availability of human capital and skill-set of the talent pool in Albania;
- During June 2019, we conducted 16 structured interview sessions with companies operating in the BPO industry being our main scope, as well as Telecommunication, Banking, ICT and Healthcare.

The number of BPO companies interviewed comprises 4 companies, followed by 3 companies in each of the BPO-ICT, Banking and Telecommunication sector. Moreover, we interviewed 2 Government Institutions and 1 Healthcare Tourism company.

The industries were selected with the assumption that they are representative of a wider group of Albanian companies, which business activities rely heavily on personal data processing and consequently, are more exposed and interested on the impact and implications of GDPR implementation in Albania.

In order to generate a uniform information from the interviews with selected companies operating in abovementioned industries, we designed a standard and structured set of questions to serve as a reference during our interviews. Yet, the group of questions were differentiated to address two main categories: BPO and non-BPO industry companies. The questions aimed to collect information

on the general awareness of interviewed companies, on the implications of GDPR implementation on their business performance, their level of preparedness in terms of capabilities, knowledge, expertise and governance of the compliance with current local legislation and future GDPR implementation. The scope of the interviews included also whether the GDPR awareness and any potential actions undertaken by the interviewed companies were driven by compliance requirements from their contractors/business partners as well as whether they have undertaken any level of preliminary assessment on potential challenges and benefits of future GDPR adoption into Albanian legislation on data privacy.

The questions were structured, to lead to the core matter, whether the GDPR implementation in the EU countries has posed any challenges for their current business performance including also job reduction or creation. Further to this, we asked the companies whether they already posses the expertise needed for GDPR implementation and their plans related to staff trainings. We also analyzed whether the future implementation of GDPR in Albania shall influence their performance in terms of increase of current services volume or expansion of the range of services and therefore the creation of new jobs.

We considered the fact that multiple answers from professionals working in the same company will affect the accuracy of the research. As per this, when meeting the companies' representatives, we concentrated in one representative per company and mainly in those functions responsible for data privacy or when such role is not in the structure of the Company, we have interviewed the Managing Directors/Administrators.

We targeted an initial pool of companies and organizations to be interviewed. However, due to their limited awareness and knowledge in the GDPR as well due to confidentiality reasons in some other cases, we interviewed only 71.4 percent of the targeted pool. The experiences of the interviewed professionals vary from five to more than ten years, and 30.8 percent of the interviewees were Administrators/General Managers, 53.8 percent of the interviewees were Legal and/or Compliance Managers and only 15.4 percent were HR Managers. They are working for small, medium and large size companies, depending on the number of employees.

3. REPORT

3. 1. Potential impact from GDPR enforcement in the Albanian business environment

This Part # 1 of the Report provides an analysis of the current and future legal situation in the field of personal data protection in Albania. The analysis contains a comparative overview of the provisions of Albanian legislation *vis-à-vis* those of GDPR.

3. 1. 1. GDPR

The material scope of GDPR comprises the processing of personal data through automated means and through other forms of processing, which are part of a filing system or are intended to form part thereof.

The territorial scope of GDPR (introduced in article 3 thereof) relates to the activities of an establishment of a data controller or data processor in the EU, regardless if the processing occurs or not in this territory.

In addition to that, it states that the provisions of GDPR apply also to the processing of personal data of data subjects who are in the EU, by a data controller or data processor not established in such jurisdiction, where the mentioned activities are related to:

(i) The offering of goods or services to the data subjects in the EU; or

(ii) The monitoring of their behavior as far as their behavior takes place in the EU.

A '*controller*' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

A '*processor*' means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller means.

The personal data are defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

According to article 5 of GDPR, the processing of personal data shall be based on the following principles:

(a) '*Lawfulness, fairness and transparency*', which means that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject;

(b) '*Purpose limitation*', which means that personal data shall be collected for specified, explicit and legitimate purposes and not further

processed in a manner that is incompatible with those purposes;

(c) '*Data minimisation*', which means that the personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) '*Accuracy*', which means that the personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) '*Storage limitation*', which means that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

(f) '*Integrity and confidentiality*', which means that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

(g) '*Accountability*', which means that the controller shall be responsible for, and be able to demonstrate compliance with points (a) to (f) above.

Moreover, article 6(1) of GDPR states that the processing of personal data shall be considered lawful, only if (at least) one of the following cases applies:

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

GDPR confers special focus onto processing of special categories of personal data, as per article 9 thereof, which comprise the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of biometric data for the purpose of uniquely identifying a natural person, and health or sexual life/orientation related data.

Among this category of personal data is to be noted the inclusion of the following subcategories:

(i) “genetic data” meaning “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question”; and

(ii) “biometric data” meaning “personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”.

The processing of the special category of personal data is (principally) prohibited. However, article 9(2) of GDPR provides for the relevant cases when such processing might occur, which include, *inter alia*, the explicit consent of data subjects, the processing is necessary for purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and social security and social protection law, the processing is necessary to protect the vital interest of the data subject or of another natural person (where the data subject is physically or legally incapable of giving consent), processing relates to personal data manifestly made public by the data subject, processing is necessary for establishment, exercise or defense of legal claims, the processing is necessary for reasons of public interest or for purposes of preventive or occupational medicine or for reasons of public interest in the area of public health, etc.

In addition to the above, a special emphasis is given to the processing of personal data relating to criminal convictions and offences (article 10). In this regard, GDPR sets out that the processing based on article 6(1) (as indicated above) of GDPR shall be carried out only under the control of the official authority or when the processing is authorized by the EU or a member state law providing for appropriate safeguards for the rights and freedoms of the data subjects.

In case the processing of personal data is based on the consent of data subject, any data controller should meet the conditions laid down under article 7 of GDPR. The controllers should be able to demonstrate that the data subject has consented to processing of the relevant personal data (i.e. accountability principle).

The same article requires that, in case the consent is given in the context of a written declaration which also concerns other matters (i.e. service agreement, employment agreement, etc.), the request for consent shall be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Otherwise, any part of such a declaration that infringes the provisions of GDPR shall not be binding.

In any case, the data subject should be informed about his/her right to withdraw the granted consent at any time; such withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.

As a 'general rule', it should be as easy to withdraw as to give consent.

Furthermore, GDPR provides for specific provisions dealing with the conditions of consent applicable to children in relation to information society services. In this view, article 8 of GDPR stipulates that in case of processing based on the consent of data subject, in relation to the offer of information society services to a child, such processing shall be lawful only if the child is at least 16 years old. In case the child is younger than 16 years old, the consent given or authorized by the holder of the parental responsibility over the child is necessary; otherwise, the processing shall be considered unlawful.

As regards the minimum age, GDPR grants discretional room to the member states to provide for a lower age, provided that is not below 13 years.

In addition to the above, in the below subsections of this section of the Report will be provided a general overview of the following main areas of the GDPR:

- Rights of data subjects;
- Data controller and data processor;
- Persona data security;
- Data protection officer;
- International transfer of personal data.

3.1.2.1 Rights of data subject

GDPR confers onto the data subject a wide range of rights related to the processing of their personal data. Such rights, on the other hand, are to be considered as obligations of data controllers toward the data subjects themselves and toward the (relevant) supervisory authority in relation to the compliance with the provisions of GDPR.

Pursuant to article 12 of GDPR, the data controller is obliged to take appropriate measures to provide any information to the data subject, in relation to the processing of his/her personal data in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*" (in particular, for any information addressed specifically to a child). The same article requires that the information should be given in written, or by other means (including electronic means, where appropriate). In addition, the mentioned information might be given also orally, if the identity of the data subject is proven by other means.

In terms of time, GDPR provides that the information/action requested by the data subject should be given/taken without undue delay and in any case within one month upon receipt thereof (i.e. extendable to three months, dependent on the complexity and number of requests).

The same term applies also regarding the information of the data subject for the information that cannot be given or

action that cannot be taken by the data controller. In such case, the refusal to address the relevant request should be accompanied by the respective reasons thereof and information on the possibility of lodging a complaint with the supervisory authority and seeking a judicial remedy.

A summary of the main rights of the data subjects (i.e. laid down in Chapter III of GDPR) is found in the below subsections.

I. Right of information

As regards this topic, GDPR differs between two forms of information to be provided, as follows:

- Information related to data processed (collected) from the data subject (direct processing) – article 13;
- Information related to data not processed (collected) from the data subject (indirect processing) – article 14.

In addition to as indicated in section 3.1.2. above, in case of personal data collected directly from the data subject, according to article 13 of GDPR, the data controller shall provide the data subject with, *inter alia*, the following information:

(i) The identity and the contact details of the controller (and/or the latter's representative);

(ii) The contact details of the Data Protection Officer, where applicable;

(iii) The purposes of the processing and the legal basis thereof;

(iv) The legitimate interests pursued by the controller or by a third party, where applicable;

(v) The recipients or categories of recipients of the personal data (if any);

(vi) The information on international transfer of personal data to a third country or international organization and the information about the existence or absence of an adequacy decision by the EU Commission that entitles such transfer, where applicable. In case the personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer and obtain a copy of such data (if they have been made available).

(vii) The personal data retention period or, if that is not possible, the criteria used to determine such period;

(viii) The information on the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(ix) The information on the right to withdraw consent at any time (where applicable), without affecting the lawfulness of processing based on consent before its withdrawal;

(x) The information whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the

personal data and of the possible consequences of failure to provide such data;

(xi) The information on the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

In case of change of the purpose of the processing, the data controller should inform the data subject (prior to the further processing of his/her personal data) on such other purpose, as well as provide to him/her with the information indicated in points (vii) to (xi) above.

In addition to as indicated in section 3.1.2. above, in case of personal data collected not directly from the data subject (i.e. indirect processing), according to article 14 of GDPR, the data controller shall provide the data subject, *inter alia*, with the information about the source where the personal data originate, as well as with the information indicated in points (i) to (ix) and (xi) above.

The information regarding the personal data that are not directly collected from a data subject, should be delivered to the latter within a reasonable period after obtaining the personal data (i.e. but at the latest within one month, having regard to the specific circumstances related to the data processing), or at least at the time of first communication with the data subject (i.e. if the personal data are to be used for communication with the latter), or, if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

II. Other rights

Articles 15 to 22 of GDPR provides for a set of entitlements of data subject as regards the processing of his/her personal data.

Such rights include the following:

- Right to access: The same information rules as indicated in subsection 3.1.2.1 above apply also in case of request of data subject to access the personal data being processed by a data controller (article 15). Moreover, the data controller is obliged provide to the data subject a copy of the personal data that are being processed.
- Right to rectification: According to this entitlement, the data subject has the right to seek and obtain the rectification of inaccurate and/or incomplete personal data without undue delay.
- Right to deletion/right to be forgotten: The data subject shall have the right to obtain from data controller the erasure of personal data concerning him/her (the right to be forgotten). Following the request of a data subject, the controller is obliged to erase personal data without undue delay, inter alia, in case the personal data are no longer necessary for the purposes they were collected/processed, the data subject objects the processing of personal or withdraws consent on which the processing is based, the personal data have been unlawfully processed, etc.

In case the data controller has made the personal data public and is obliged to erase the personal data, the latter (taking account of available technology and the cost of implementation) shall take reasonable steps to inform (other) controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

- Right to object to processing: The data subject has the right to object the processing of personal data, if the basis for such processing is either the public interest or legitimate interest of the controller or of a third party. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing, which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- Right to restrict processing: The data controller should restrict the processing of personal data, inter alia, if the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of personal data, the processing is unlawful (in such case instead of erasure, the data subject might requests the restriction of processing), etc.
- Right to data portability: According to this entitlement, the data subject has the right to receive his/her personal data (which he/she has provided to a controller) in a structured, commonly used and machine-readable format and also the right to transmit such data to another controller, if, inter alia, the processing is based on the consent of the data subject or on a contract and the processing is carried out by automated means.
  In exercising his/her right to data portability pursuant to the above, the data subject shall have the right to have the personal data transmitted directly from one controller to another, if this is technically feasible.
- Right to withdraw consent: GDPR stipulates that the data subject is entitled to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before such withdrawal.
- Right to object and automated individual decision-making: The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of his/her personal data which is based on point (e) or (f) of Article 6(1)2 of GDPR, including profiling based on those provisions.
  According to article 22, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or, similarly, significantly affects him/her.

[2] (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The right to object should be explicitly notified to the data subject (i.e. presented clearly and separately from any other information), at the latest, at the time of the first communication with the data subject.

- Right to object to direct marketing: The provisions of the GDPR set out that in cases when personal data are (being) processed for direct marketing purposes, the data subject is entitled to object, at any time, to (further) processing of his/her personal data for such purpose; this includes also profiling, to the extent that it is related to such direct marketing.
  The right to object to direct marketing should be explicitly notified to the data subject (i.e. presented clearly and separately from any other information), at the latest, at the time of the first communication with the data subject.

3.1.2.2 Data controller and data processor

Data controllers play the key role in the processing of personal data. They are at the center of this process and, on the other hand, the entire process is tailored to fit and serve to the activities of the latter. To this effect, GDPR provides for several responsibilities and obligations pertaining to the data controllers.

In this view, the data controllers are obliged to establish and implement the appropriate technical and organizational measures the enable the processing of personal data in accordance with GDPR. These measures, include, but are not limited to, the implementation of appropriate security policies, adherence to the codes of conduct applicable to the relevant industry or certification of their processing systems through certification mechanisms.

In any case, the data controller is also obliged, at any time, to ensure protection of personal data 'by design' and 'by default'.

This means that the latter should have in place and implement technical and organizational measures (i.e. pseudonymisation, etc.) that are designed to effectively implement data-protection principles (such as data minimization) and to vest the processing itself with the necessary safeguards in order to protect the rights of data subjects and also comply with GDPR requirements.

Moreover, the mentioned technical and organizational measures of the data controller should, by default, ensure that the processing of personal data is limited to the processing of personal data that are necessary for each specific purpose of the processing. This obligation relates to the amount, extent, retention period and accessibility of personal data processed. These measures must ensure that (by default) the access to personal data is not granted to an indefinite number of individuals, without the individual's intervention.

The data controller might conduct personal data processing itself and/or through engagement of data processors, who carry this out on behalf of the data controller.

In case of engagement of data processors, the controller should ensure that such processors provide sufficient guarantees to implement appropriate technical and organizational measures for purpose of complying with the GDPR requirements and protection of data subjects' rights.

The engagement of a data processor should be done, *inter alia*, in virtue of a contract to be concluded between the latter and the data controller, containing the duration, nature and purpose of processing, the personal data types and data subjects categories. In addition, to that, article 28 of GDPR provides also for other requirements that should contain the contract between the data controller and data processor. According to article 28, the contract should set out that the data processor:

(i) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing;

(ii) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(iii) takes all measures required pursuant to the provisions of GDPR on security of data;

(iv) respects the conditions referred above on engaging another processor.

As this is concerned, according to GDPR the processor shall not engage another processor without prior specific or general written authorization of the controller;

(v) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to address to requests for exercising the data subject's rights;

(vi) assists the controller in ensuring compliance with the obligations pursuant to the provisions of GDPR on security of data, taking into account the nature of processing and the information available to the processor;

(vii) at the choice of the controller, deletes or returns all the personal data to the controller after the termination of the processing service, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(viii) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in article 28 (*Processor*) of GDPR and allows for and contributes to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

Furthermore, the data controller is obliged to maintain in written (including in electronic form) a record of

processing activities under its responsibility, containing, *inter alia*, the information about the name and contact details of the controller, controller's representative and data protection officer, the purposes of personal data processing and a description of the categories of data subjects and those of personal data, etc.

Almost the same applies also to the data processor, who should maintain written record of all processing activities performed on behalf of a data controller, which should include the name/contact details of the data processor and those of the relevant data controller, categories of processing, international transfer, etc.

GDPR provides also for a threshold, which determines the enterprises/organizations that are obliged to keep the records of processing activities. Pursuant to article 30 of GDPR, the obligation applies to enterprises/organizations having 250 or more employees. The enterprises/organizations that do not meet this threshold are not bound by this obligation, unless the processing of personal data is likely to result in risk to the rights and freedoms of data subjects, the processing is not occasional, or it includes categories of (sensitive) data provided for under articles 9(1) and 10 of GDPR.

In relation to the obligation to compensate the data subject for the damage caused, article 82 of GDPR sets out that the latter are entitled to receive compensation from the controller or the processor for the damage incurred (as a result of an infringement of the provisions of GDPR).

As a rule, in the first line of liability to compensate the persons having suffered damages from the infringement of the provisions of GDPR appears to be the data controller. Whilst, the data processor shall be held liable for the damage caused only if it has not complied with the obligations that GDPR has set out specifically for the processors and if it has acted outside or contrary to lawful instructions of the data controller.

3.1.2.3 Personal data security

GDPR dedicates a separate section of provisions to the obligations of the data controllers/processors to guarantee the security of personal data processing.

The data controllers/processors are obliged (taking into account, among the others, the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, the related risks, etc.) to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, *inter alia*, as appropriate the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and

organizational measures for ensuring the security of the processing.

In assessing the appropriate level of security, the data controllers should take into account, in particular, the risks accompanying the processing; especially, those related to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

In this context, dependent on the type of processing (including, in particular, the using of new technologies), the data controller, prior to commencement of the processing of personal data, should carry out an assessment of the impact of intended processing operations on the personal data protection. The impact assessment, in particular, is required in case of automated processing, processing on a large scale of special categories of personal data as per article 9(1) and 10 of GDPR, etc.

GDPR obliges the supervisory authority to establish and make public a list of processing operations that should undergo the impact assessment.

In addition, article 36 of GDPR provides for the obligation of the controller to consult the supervisory authority prior to commencement of personal data processing, in case the relevant data processing impact has shown that the processing might result in a high risk in absence of the measures to be taken by the controller to mitigate such risk.

As an element for demonstrating compliance with security requirements are considered also the adherence to an approved code of conduct or an approved certification mechanism as referred to, respectively, under articles 40 and 42 of GDPR.

Article 40 of GDPR provides for the possibility of controllers/processors to prepare and adhere to the codes of conducts that are intended to contribute to the proper application of the provisions of GDPR, by taking into account the specific features of different sectors and the specific needs of micro, small and medium sized, enterprises.

The code of conduct represents an instrument that might be drawn up by associations (or other bodies) representing categories of data controllers/processors, for purpose of complying with GDPR, in relation to, but not limited to, the fair and transparent processing, legitimate interest pursued by controllers in specific contexts, the collection of personal data and their pseudonymisation, the exercise of rights of the data subject, international transfer to third countries, etc.

Interesting is the fact that according to article 40(3) of GPDR, the codes of conduct might be adhered also by the data controllers/processors that are not subject to GDPR (for, example Albanian controllers/processors), in order to provide appropriate safeguards within the framework of international transfer of personal data. These (out of jurisdiction) controllers/processors shall make binding and enforceable commitments via contracts or other legally binding instruments.

The final approval of the codes of conducts is to be carried out by the supervisory authority, based on its

opinion whether the provisions thereof are compliant with GDPR.

On the other hand, article 42 encourages the establishment of data protection certification mechanisms, seals or marks, for purpose of demonstrating compliance with the GDPR provisions. To this effect, GDPR sets out that the specific needs of micro, small and medium-sized enterprises should be taken into account.

The certification should be voluntary and should be issued for a maximum period of three years. In any case, it does not reduce the responsibility of the data controller/processor to comply with GDPR provision and also does not affect the supervision powers of the supervisory authority.

The bodies entitled to issue the certificates should be accredited by the competent supervisory authority and/or the national accreditation body. They shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with GDPR. The accreditation shall be issued for a maximum period of five years.

Same as in case of codes of conduct, certification mechanisms, seals or marks, may be established for purpose of demonstrating compliance with GDPR (i.e. existence of appropriate safeguards) of data controllers/processors that are not subject to GDPR itself (for example, Albanian controllers/processors) within the framework of international transfer of personal data. Again, such (out of jurisdiction) controllers/processors shall make binding and enforceable commitments via contracts or other legally binding instruments.

Beside the above, a special emphasis is dedicated to the notification obligations in case of personal data breach. To such an end, in the case of a personal data breach, the controller shall without undue delay (however, not later than 72 hours) notify the personal data breach to the supervisory authority competent. If the notification is not made within the foregoing deadline, it shall be accompanied by reasons for the delay.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The notification of the controller shall describe the nature of the personal data breach, communicate the name/contact details of the data protection officer or other contact point where more information can be obtained, describe the likely consequences of the personal data breach and the measures taken (or proposed to be taken) by the controller to address the personal data breach.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with GDPR.

Infringements and breaches of GDPR provisions shall be subject to administrative fines up to EUR 20 000

000, or in the case of an undertaking, up to 2 - 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

3.1.2.4 Data Protection Officer

Article 37 Of GDPR provides that the controller and the processor shall appoint a Data Protection Officer (DPO), if one of the following applies:

(i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(ii) the core activities of the controller/processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(iii) the core activities of the controller or the processor consist of processing on a large scale of special categories of (sensitive) data provided for under articles 9 and 10 of GDPR.

The contact details of DPO shall be published and communicated to the supervisory authority as well.

The DPO might be an employee of the controller/processor or a third party service provider. GDPR provides also that a group of undertakings might appoint a single DPO, provided that the latter is easily accessible from each undertaking of the group. In cases other than those indicated in points (i) to (iii) above, a controller/processor or associations thereof shall appoint a DPO if required by the EU or the Member State law.

According to GDPR, the DPO is a key person and plays a very important role in assuring compliance with the provisions thereof. Hence, the data controller/processor are obliged to support the DPO in performing the tasks assignment to him/her and provide the necessary resources for performing such tasks. DPO should be free of the instructions of the data controller/processor that has appointed him/her and he/she should directly report to the highest management level of controller/processor.

The DPO shall serve as the 'face' of the controller/processor toward the data subjects (who might contact him/her with regard to, *inter alia*, exercise of their rights under the GDPR) and toward the supervisory authority.

As regards the criteria on appointment of the DPO, GDPR is too generic when stating that the latter should be appointed based on his/her professional qualities and, in particular, expertise level of knowledge of data protection legislation.

According to article 39 of GDPR, the DPO shall carry out at least the following tasks:

(i) Inform and advise the controller/processor and the employees, who carry out processing, about their obligations pursuant to the data protection legislation (i.e. GDPR and to other Union or Member State data protection provisions);

(ii) Monitor compliance with data protection legislation and with the policies of the controller/processor, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(iii) Provide advice where requested as regards the data protection impact assessment and monitor its performance;

(iv) Cooperate with the supervisory authority and act as the contact point for the latter on issues relating to processing.

3.1.2.5 International transfer of personal data

The rules and criteria on international transfer of personal data are laid down in articles 44 to 50 of GDPR. It does not provide for any specific definition of 'transfer'. However, the general understanding is that international transfer of personal data means to move such data through communication, disclosure or making them available otherwise from the sender to a recipient in another country.

The transfer of personal data to third countries might take place in one of the following options:

(i) Transfer on the basis of an adequacy decision;

(ii) Transfer subject to appropriate safeguards;

(iii) Transfer based on derogations for specific situations.

I. Transfer based on an adequacy decision

The transfer of personal data to a third country (or an international organization) may take place, if the EU Commission has decided that such third country/organization ensures an adequate level of protection of personal data (article 45).

The adequate level per personal data protection represent the principal condition that enables the transfer of personal data to third countries/international organizations.

The adequacy of a country is decided by decision of EU Commission, by taking into account, *inter alia*, the rule of law and respect for human right in the said country, the existence and effective functioning of (at least) one independent supervisory authority, the international commitments undertaken by the said country, etc.

II. Transfer subject to appropriate safeguards

Should a third country or international organization not be subject to an adequacy decision on the part of EU Commission, then the controller/processor might transfer the personal data to such third country/international organization only if the latter has provided the appropriate safeguards, as well as on the condition that to the data subjects are guaranteed enforceable rights and effective legal remedies.

The mentioned appropriate safeguards might be provided for by the following acts:

(i) A legally binding and enforceable instrument between public authorities or bodies;

(ii) Binding Corporate Rules;

(iii) Standard data protection clauses adopted by the EU Commission;

(iv) Standard data protection clauses adopted by a supervisory authority and approved by the EU Commission;

(v) An approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(vi) An approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

The existence of the above listed safeguards does not require any specific authorization from a supervisory authority.

The above safeguards might be also provided through (i) contractual clauses between the controller/processor and the recipient situated in the third country/international organization or (ii) provisions to be inserted into administrative arrangements between public authorities or bodies, which include enforceable and effective data subject rights. In such cases, the authorization of the supervisory authority is also needed.

A special attention is attributed to the appropriate safeguards provided through the Binding Corporate Rules ("BCR").

According to Article 4(20) of GDPR, the BCR represent personal data protection policies that are adhered to by a controller/processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Based on the above definition, is to be noted that BCR applies to two cases:

(a) in case of transfers within a group of undertakings. Whereby GDPR defines the 'group of undertakings' as "*a controlling undertaking and its controlled undertakings*"; or

(b) a group of enterprises conducting a joint economic activity. Where by the 'enterprise' is defined as "a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity".

III. Transfer based on derogations for specific situations

Article 49 of GDPR provides for the derogations that apply to specific situations of international transfer, if the country/international organization where the personal data shall be transferred to is not subject to any adequacy decision or there are not appropriate safeguards in place with the recipients situated in third countries.

Such derogations include one of following cases:

(i) The data subject has explicitly consented to the proposed transfer (i.e. after having been informed of the possible risks of such transfers, due to the lack of an adequacy decision and appropriate safeguards);

(ii) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(iii) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iv) The transfer is necessary for important reasons of public interest;

(v) The transfer is necessary for the establishment, exercise or defense of legal claims;

(vi) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(vii) The transfer is made from a register intended to provide information to the public and which is open to consultation by the public in general or by any person who can demonstrate a legitimate interest.

The transfer of personal data in virtue of the above derogations is to be considered as *ultima ratio* solution. They relate to specific situations, not to an established routine of transfer of personal data to third countries.

3. 2. PART # 2 –The economic sectors that will be affected by the implementation of GDPR

This Part # 2 of the Report comprises the legal and economic perspective of sectoral impact that the implementation of GDPR would have in Albania. It contains also two separate sections dealing with ICT and information security impact.

As regards the legal perspective, the analysis is limited to the immediate effect of GDPR implementation to specific sectors of economy that have been subject to specific regulation on the part of the Commissioner.

The economic prospective analyses the impact of the GDPR on a high-level cost benefit analysis on several sectors or industry profiles. As such, it is provided a description of the main sectors of the Albanian economy, which are dependent on personal data and, at the same time, introduces the main effects of the GDPR.

The purpose of our approach is to identify the costs and benefits that are likely to occur from the implementation of the GDPR, and the likely economic impact on businesses and consumers. The analysis is mainly focused on qualitative data, using case studies and international reference analysis, considering short-term as well as long-term effects.

As mentioned above, this part of the Report provides an analysis regarding information security and ICT sector, which includes an overview of main GDPR requirements that might demand technology innovation within organizations. Further, it is described how this sector might be impacted from GDPR.

3. 2. 1. Legal perspective

The Commissioner has issued several instructions dealing with the processing of personal data in specific sectors, such as education, healthcare, direct marketing, journalism, hotel services, telecommunications, and banks.

In addition, the Commissioner has also enacted other acts dealing with, *inter alia*, the processing of personal data for employment purposes in private sector.

All these instruments introduce and articulate, based on the general and/or specific rules of the Albanian legislation on personal data protection, the Commissioner's approach for each of the abovementioned areas.

The rights and obligations stipulated under these sublegal acts are without prejudice to the provisions of the Law on Personal Data Protection and other acts of Commissioner having general (cross sectoral) effects over data controllers/process irrespective of the sector of their activities.

On the other hand, under chapter IX of GDPR are laid down specific provisions related to specific processing situations, such as journalistic purposes, processing of the national identification number, or processing in the context of employment, etc.

This section 3.2.1 provides a summary of the sectoral acts of the

Commissioner and a summarized high-level assessment on eventual impact of transposed GDPR provisions onto such sectors.

3.2.1.1 Processing of personal data in education sector

The processing of personal data in education sector is subject to specific rules set out through the following instructions:

(i) Instruction no. 4, dated 16.03.2010 "On personal data security measures in the field of education activities" as amended; and

(ii) Instruction no. 7, dated 09.06.2010 "On personal data processing in the University Education Institutions" as amended.

Both instructions provide for rules to be complied with the by the pre-university and university education institutions.

They reemphasise the obligations of the data controllers (i.e. education institutions) for carrying out the lawful processing of personal data, including, but not limited to, the proper information to data subjects (i.e. students) regarding the categories of personal data, the purpose of processing and the retention period and deletion obligations if the data are not necessary anymore.

Further, they contain detailed rules on security of personal data, based, *inter alia*, on confidentiality and integrity of the processing operations, as well as rules on international transfer of personal data.

All education institutions should comply with the provisions of the Law on Personal Data Protection[3].

3.2.1.2 Processing of personal data in healthcare sector

Personal data processing in healthcare sector is governed by the following specific acts of the Commissioner:

(i) Instruction no. 5, dated 26.05.2010 "On essential rules in relation to protection of personal data in the healthcare system" ("Instruction no. 5"); and

(ii) Instruction no. 23, dated 20.11.2012 "*On processing of personal data in the healthcare sector*" ("Instruction no. 23").

The processing of personal data in healthcare system is based on the following three main principles:

1. Any patient has the right to privacy and confidentiality of his/her health information (i.e. sensitive data);

2. Any patient is entitled to have control over the disclosure of his/her health information, through the provision of his/her clear consent and withdrawal of such consent;

3. For any non-consented disclosure of the confidential information on the part of healthcare professionals should be considered the

[3] As indicated in each subsection of section 3.1.1 above.

indispensability of such disclosure, the proportionality and the related risks.

The healthcare professionals should properly inform the data subjects (i.e. patients) about the their rights related to processing of their personal data to be used for healthcare purposes, as well as in relation to the secondary use of personal data of the latter, which use is not directly connected to the provision of healthcare services.

In both cases, the clear and written consent of the patient is mandatory.

In addition, the instructions provide for specific rules regarding the disclosure of health information (i.e. including the factors that should be considered in case of, *inter alia*, disclosure of personal data without consent of the patient), archiving/files of patients, retention period, transmitting of data to third parties and international transfer, as well as the procedures on processing of personal data in case of termination of healthcare destruction of archiving means, etc.

3.2.1.3 Processing of personal data in journalistic sector

The processing of personal data for journalistic purposes is subject to, *inter alia*, Commissioner's instruction no. 9, dated 15.09.2010 "*On the essential rules related to the protection of personal data in printed, visive and audio-visive media*".

This instrument provides for rules related to privacy of data subjects with regard to journalistic publications. As such, the mass media should account to the right of the citizens on private and familiar life, health and correspondence. It states that the journalists cannot access the private life of the individuals without their consent. In addition, special focus is awarded to the publications that involve sensitive data, photographs, private property, criminal proceedings and child protection, etc., from journalistic activities.

3.2.1.4 Processing of personal data in banking sector

The personal data processing on the part of the banks and/or non-banking institutions in the Republic of Albania during the performance of their banking/financial activity is done, *inter alia*, in accordance with Commissioner's Instruction no. 20, dated 03.08.2012, "*On the personal data processing in the banking sector*".

According to this instrument, the banks are entitled to collect only the personal data of their client and/or third-party contractors for purpose of their commercial activity and which are necessary for carrying out the activities that they have been licensed for by the Bank of Albania, or for the fulfilment of their needs as commercial legal entities.

As regards the features of the consent of the clients, the instruction makes direct reference to the relevant provisions of the Law on Personal Data Protection[4].

[4] See section 3.1.1 and subsection 3.1.1.1 above.

In addition, this act sets out rules related to the retention period of personal data, requirements on security measures on personal data protection, right to file complaint to the Commissioner, etc.

3.2.1.5 Processing of personal data in sector of hotel services

The rights and obligations of hotel operators in relation to personal data processing are contained, *inter alia*, under Commissioner's instruction no. 10, dated 06.09.2011 "*On personal data processing in the ambit of hotel services*".

The instruction sets out that the personal data should be processed in accordance with the Law on Personal Data Protection.

The hotel operators should use the personal data solely in relation to the services provided by them. The processing of personal data for other purposes (including, but not limited to, direct marketing) should be processed only if the respective data subject (i.e. client) has granted his/her consent to such an end.

In addition, this instruction contains rules on retention period and processing means of personal data, as well as the list of such data that might be collected by the hotel operator for booking purposes. A special attention in this regard is paid to the collection and further processing of ID cards, passports or other travel documentation. To this effect, the instruction requires that the data subject has given his/her explicit consent as per the standard consent form attached to such act.

3.2.1.6 Processing of personal data in telecommunication sector

Instruction no. 14, dated 22.12.2011 "*On processing, protection and safety of personal data in the public electronic communication sector*" applies to personal data processing in the ambit of electronic communications.

It intends to ensure the protection of personal data by taking into consideration and guaranteeing the free movement of the data and telecommunication service means in the country.

The processing of personal data in telecommunication sector should be based on specific, clear and lawful purposes. The processing for other purposes (i.e. direct marketing, etc.) is not allowed, unless explicitly consented by the data subject.

The processing of personal data should be based on the principle of data minimization, and in accordance with other principles applicable to the protection of personal data. Thus, the telecommunication operators should take the appropriate technical and organizational measures to protect the personal data from accidental or unlawful destruction, accidental loss, unauthorized access, unlawful disclosure, etc.

In addition, the instruction sets out rules on personal data retention, confidentiality and security of personal data.

3.2.1.7 Processing of personal data for direct marketing

The processing of personal data for direct marketing purposes finds specific regulation under the following acts of the Commissioner:

(i) Instruction no. 16, dated 26.12.2011 "On protection of personal data in the direct marketing and the safety measures" as amended;

(ii) Instruction no. 6, dated 28.05.2010 "On correct use of SMS for promotional, advertising, information, direct sales, by means of mobile telephony"; and

(iii) Instruction no. 14, dated 22.12.2011 "On processing, protection and safety of personal data in the public electronic communication sector".

When processing personal data for marketing purposes, the data controllers are obliged to inform the data subjects on the identity of the controller, purpose of the processing, their rights to access, correction, and other related rights, as well as about their right not to undergo processing of personal data for marketing purposes and to object such processing, the receivers of their personal data and the right to object transmitting, etc.

As indicated under subsection 3.1.3.2 above, in case of direct marketing, the controllers are obliged to provide to data subject the mandatory information relating to processing of personal data, even when such data are not directly collected from the latter.

In addition, the instructions provide for processing of minors' personal data (i.e. upon consent of the parent), security measures, confidentiality, and rules on use of short message services (SMS) for promotional/marketing purposes, etc.

3.2.1.8 Processing of personal data for employment purposes in private sector

The processing of personal data for employment purposes is governed, *inter alia*, by the provisions of Commissioner's instruction no. 11, dated 08.09.2011 "*On processing of personal data of the employees in the private sector*" as amended.

The provisions of this instruction apply to the recruiting phase (i.e. pre-hiring) and during the existence of the employment relationship (i.e. hiring phase).

Same as in other sectors and/or purposes of personal data processing, the processing for employment purposes should be based on the principle of data minimization, purpose limitation and storage limitation (i.e. to the extent that the personal data are necessary for the relevant employment relationship).

The present act contains also rules related to processing of sensitive data (i.e. especially in the ambit of health and safety measures/medical examination), consent of the employee, information to be given to the latter regarding the processing of their personal data, security measures, monitoring of working areas, use of biometric data, retention period, etc.

3.2.1.9 GDPR's sectoral related provisions

Chapter IX of GDPR contains provisions relating to specific personal data processing situations. These provisions include, *inter alia*, the processing for journalistic purposes, the processing of national identification number, the processing in the context of employment, etc.

As regards the processing for journalistic purposes, article 85 of GDPR sets out that the right of protection of personal data as per GDPR itself should be reconciled with the right to freedom of expression and information (i.e. including journalistic purposes). It further highlights the exemptions or derogations to be provided in case of processing for journalistic purposes.

In relation to the processing of national identification number, article 87 of GDPR entitles the member states to determine the specific conditions in relation to the processing of this number. It states also that the use of the national identification number should be used only under the appropriate safeguards (as provided for under the provisions of GDPR) in relation to the rights and freedoms of the data subjects.

Concerning the processing of personal data for employment purposes, GDPR provides that the member states may stipulate (more) specific rules for ensuring the protection of the rights and freedoms of the data subjects in relation to processing of their personal data in the employment context. Such rules should include specific measures to safeguard, among the others, the human dignity and fundamental rights, with particular regard to transparency of personal data processing, the personal data transfer and monitoring systems at the work place.

3. 2. 2. Case studies: potential effects of the GDPR on several Sectors

The macroeconomic overview of the country lays a foundation to the analysis we have conducted. The overview demonstrates the constant economic growth experienced and forecasted. The labour force is educated, young; technology driven and the labour costs, when compared to other EU countries, are lower. Albania has implemented fiscal policies that tend to be supportive towards businesses especially when compared to EU countries.

GDPR will greatly affect how companies approach and manage the collection and processing of personal data. It has a far-reaching effect beyond the union's border therefor companies will have to comply with the new regulation when conducting business with EU and EU citizens.

This section summarizes an analysis of the impact of GDPR implementation in the Albanian economy particularly in industries that process a high volume of personal data such as information and communication technologies, financial industry, business process operation, healthcare and public sector. Based on studies, researches, statistics and best practice examples we have prepared a walkthrough of the information that

these industries collect and how GDPR will affect them.

In conclusion, it is expected that being GDPR compliant will in the short run bring an increase in expenditures for companies but in the long run, it will help them draw foreign costumers and build costumer trust to their brand.

Considering the recent timeframe in which GDPR is implemented in Europe there is a lack of quantitative data. Thus, the walkthrough of the impact of GDPR in Albanian specific sectors is analyzed on a qualitative rather than a quantitative basis.

I. Information and Communication Technologies (ICT) Sector

ICT refers to technologies that provide access to information through telecommunications. This industry in Albania has improved significantly in the last 6 years due to the efforts from the local government, donors and businesses. Albanian telecom market is small but with a strong competition amongst the firms. In early 2018, Plus Communication exited the market with its costumers reallocated equally to Vodafone Albania and Telekom Albania. Vodafone remains the market leader with 1.22 million active subscribers out of 2.6 million registered users as of March 2018. It is followed, at a distance, by Telekom Albania with 0.97 million active subscribers in March 2018 and the rest of the market share 0.42 million subscribers are held by Albtelecom. When it comes to internet providers, the developmental trajectory of the Albanian broadband market is on the rise with improvements in the quality of fixed infrastructure. The market has become more dynamic with competition between wireline broadband providers, as well as from dedicated mobile broadband services. The regulator reported 314,376 fixed broadband subscriptions in Albania at the end of March 2018, up from 266,200 at the end of 2016; dedicated mobile broadband accesses numbered 124,093. The wireline broadband market continues to attract new subscriptions, with alternative operators playing a key role. Albtelecom is the dominant player, with nearly 121,144 fixed broadband subscribers at end-March 2018, more than double that of next-placed Abcom, ASC, Abissnet and Nisatel are the other largest players, with Abissnet reporting the greatest y-o-y subscriber growth, and the incumbent ranked fourth in y-o-y growth terms.

ICT companies gather a considerable amount of data daily through various customer touchpoints. The law requires data collection; in addition, it is a useful method to understand customers' needs and to maintain competitive advantage. Mobile carriers have unprecedented access to their costumers' information and behavior. At the very least they keep records of all the incoming and outgoing calls, the phone numbers the call duration, how many times costumers check their mail and their physical location. Internet service providers track their costumer's internet traffic, as for the companies the browsing history is a revenue stream. Many ISP compile anonymous browsing logs and sell them to marketing companies or use them for

their internal marketing and digital marketing needs.

With the implementation of the GDPR in Albania, the ICT companies will have to take, *inter alia*, the following steps in order to be compliant:

Privacy by Design - Develop or update their systems in order to adopt to the Privacy by Design principle. The new systems should collect only the information's that are necessary to the business operation. Data stored should be segmented and separated from other systems to make sure it is not accidentally used for other purposes

- *Costumer consent* - From the implementation of GDPR companies will have to re ask for consent from the costumers. The format should be easy to understand and not overwritten with legal terms.
- *The right to deletion* - GDPR would require the Albanian ICT companies to keep its customers' data in an electronic format and should be able to provide customers a copy of their data as and when they demand it. In case costumers revoke consent and they ask for their personal data to be erased companies should comply in a timely manner.
- *Processing and storing* - Another step will be establishing new processes and modifying applications to ensure maximum data security during the acquisition, transfer, storage, and handling processes. It will also be necessary to integrate appropriate software or hardware to support security surveillance and auditing over operations involving data of EU citizens.

Considering the above, in short term, the needs for technology and staff training may be needed which may lead to extra expenditures in order for companies to comply with GDPR. Although in a long-term picture, it opens up the market for new investments from international companies and increases the brand loyalty from its customers. The increase of companies operating in Albania, is expected to impact the number of ICT professionals employed in the sector, increasing employment and increase of salary for professionals. Based on the interviews conducted, the respondents consider that the implementation of the GDPR might impact technology mainly related to additional staff training costs and investments to software (table 11 in Appendix 1). Although, it is impossible to quantify the level of capital investment at this stage, respondents are aware mainly in the need to enhance capacity building through outsourcing expertise, trainings of existing staff or hiring new employees. Therefore, c. 28.6% of the respondents think there will be an increase on the number of professionals hired after the GDPR implementation, while 71.4% think it is yet early to estimate. As per the same survey, 21.4% of the respondents believe that the staff increase due to the expansion of business post GDPR implementation, will vary from 1% to 3%, while c. 7.2% believe that the staff increase will be between 25% and 30% (table 10.1 in Appendix 1). Although, most of the companies believe that it is too early to estimate the expected staff increase, BPO-ICT sector expects the highest job creation. More specifically, two out of

three respondents in the Banking, BPO-ICT, BPO and TELCO, and the only respondent in Healthcare sector answered that it is too early to decide; one out of three respondents in Banking, BPO and TELCO responded that the staff increase will vary between 1% and 3%, while one out of three respondents in BPO-ICT sector expects 25% to 30% staff increase.

II. Financial sector

The majority of financial sector in Albania is represented by the banking sector, comprised by 16 banks, most of them being foreign owned. According to Bank of Albania, overall, most of them being foreign owned. According to Bank of Albania, overall, the financial sector has expanded its activity, with the largest growth observed in the non-resident sector and financial corporations. Within 2013-2017, the financial assets of all economic sectors grew by c. ALL 857 billion (or 14%), amounting to ALL 7,107 billion by the end of 2017. The non-resident sector financial assets expanded by ALL 412 billion over the 2013-2017 period.

The number of non-resident client accounts increased by a GAGR of 10.3%, from 20 thousand in 2015 to 34 thousand in 2018, amounting to 1.1% of the total accounts.

Financial institutions and financial industry service providers process a vast amount of personal data on a daily basis. Many of the data is confidential or even sensitive personal data. Banks use this information in their day-to-day activities in order to provide more personalized offers and targeted marketing, as well as improve client service, although currently these practices are not widespread in Albania. A more complex and integrated IT and data processing system would help use personal data more efficiently to help banks reinforce risk management through better monitoring and early warning systems.

The introduction of the GDPR is expected to affect how personal data are processed and protected. Costumers of banks or other financial institutions are protected while making it easier for them to know how and where their personal information is being used. Even though Albania is not member of the EU, if data violation is found, the financial institutions would face not only the Albanian regulatory authorities but also EU regulatory authorities, as well as execute transactions relating to EU customers.

- *Client Consent* – GDPR mandates organizations to gain consent (no automatic opt-in option) from customers about the personal data that is gathered. Individuals should be aware of the information financial institutions are holding. In addition, in the consent system, organizations must clearly outline the purpose for which the data was collected and seek additional consent if organizations want to share the information with third parties.
- *Minimization of data collected* - GDPR will lead banks to try to minimize the use and processing of costumer information since one of the pillars of compliance will be the minimization of data collected. On the other hand, in order to prevent money laundry all financial institutions must comply with Know Your Costumer guidelines that

requires them to collect copious amounts of data in form of a safeguard. Balancing the multiple regulatory guidelines that are in place and making them all work is one of the biggest challenges, since the cost of their data security platforms is expected to rise.

- *Privacy by design* – Financial service sector interacts with third-party vendors for various operations spanning credit and debit cards, transaction processing at point of sale (PoS) terminals and e-commerce sites, as well as offshore service providers for customer and tech support. Banks need to adopt data masking techniques like anonymization, pseudonymization, and encryption before sharing customer data with third parties to ensure GDPR compliance. Before onboarding new systems, technologies, or vendors, banks must identify privacy risks, so that mechanisms to protect data through effective access management can be built in right at the design phase.

According to a survey from Quint and Rogers[5], 75% of Customers will be open to share their information if the trust the institution. While in case a financial institution would be accused of unethical business practices, 48% would lose trust in the bank while 28% would switch to a new bank. These figures show the positive impact that GDPR will have in the bank-costumer relation, while in the same time being able to collect and process data. The IT legacy system of the big financial institutions made it hard and time consuming to manage all the information they had. Through the process of implementing GDPR, companies will have to go through all the personal data and keep only the ones that are necessary for their business process, which will make it easy for institutions to create customized products for its clients.

III. Business Process Outsourcing industry

Most outsourcing companies operating in Albania are franchises of international companies or collaborating with international corporates thus, they only need to further strengthen security and privacy and align them with the GDPR guidelines.

What will likely change, is the relationship between the company and the outsourcing provider. GDPR states that the controller must impose to its processor a list of obligations to follow such as imposing technical and organisational procedures on the processor, increasing communication between the two parties, and determining which party bears the risk upon non-compliance of an obligation. Compliance for both company and outsourcing firm is stricter, thus both should work on protecting each other's liability. Outsourcing firms will have to follow the regulations set by their clients in accordance with the GDPR guidelines and strengthen their security procedures to ensure there will be no data breach.

[5] Quint, M. and Rogers, D., 2015. *What Is the Future of Data Sharing? Consumer Mindsets and the Power of Brands*, Research report, Columbia Business School and Aimia.

Examining existing processes will help identify where new procedures and specialists are needed to comply with the GDPR. In addition, it will be necessary to evaluate the current technology so the outsourcing companies in Albania can determine technical requirements to cater to data security, data auditing, and data privacy needs. Identifying and dealing with blind spots is a critical part of this process that most likely will be accompanied with high cost.

According to International Association of Privacy Professionals (IAPP) annual report, 25% of EU based companies are withdrawing their operations from companies and countries that are non-compliant. Being GDPR compliant will increase the possibilities of Albanian companies to grow exponentially in the European market and take a part of this market share. At this stage of the project, it is uncertain how the workflow of the GDPR process implementation and how it will affect the business structure and strategy of companies in the short and long run. Therefore, it might be not possible to quantify the economic impact during the process and post-implementation. Such analysis is also supported from the survey we conducted, when more than 71.4 % of the respondents said that it was too early to estimate a figure for the financial impact of the company. Whereas more than 14.3% believed there would be more opportunities to expand the business even though they cannot yet put a figure on the size of the expansion. The remaining 14.3% had already implemented GDPR (table 10.2 in Appendix 1).

IV. Healthcare sector

The healthcare industry in Albania is developing vastly and quickly. The Albanian State healthcare system is divided into three tiers of service, namely:

i. Primary health care - includes health and hygiene centres, health education centres, maternity and paediatric clinics, local emergency rooms and rural hospitals.
ii. Secondary care - consists of medical and diagnostic services in hospitals and polyclinics.
iii. Tertiary care - consists of scientific research medicine including four national university centres with diagnostic services.

The private healthcare sector in Albania is developing, and it covers most of the pharmaceutical and dental services as well as some clinics for specialized diagnoses, mainly located in Tirana.

The industry is starting to feature modern technologies, tools, and equipment to collect as much information about patients as possible, with “big data” appearing as the new trend. The private sector collects data from its patients and records them on its database for further processing based on its needs. While the public sector is depended from the Department of Health, Information Technology and Communication's whose mission is the collection, unification and analysis of all data and health information, the use and dissemination of effective and contemporary strategies of communication and health information with the ultimate aim of improving the

quality of planning, research and healthcare service. This department is functionally involved in the Data Warehouse of the Health Information System in Albania.

- *Consent and minimize data collection* - The data collected by this industry are sensitive in nature and extremely confidential, thus the emphasis is on security and safety of the databases. Healthcare centres should ask for consent from patients to record their personal data and only collect the personal data that are needed for preventative medicine or work purposes, work capacity assessment of the worker, medical diagnosis, provision of health or social care or treatment, or managing the health and social care systems.
- *Privacy by design systems* - In order to be compliant with GDPR hospitals will invest in IT staff and new more encrypted systems, which directly translates in more investments.
- *Right to deletion* - Based on the criteria laid out by the regulation the costumer should have knowledge of the personal data collected and have the possibility to ask for the data to be erased. This requirement will make personal data's held by hospitals to be more organized thus becoming more efficient in the day-to-day use.
- *Data portability* - The portability of the data will bring ease when switching hospitals. The healthcare industry involves not only providers and physicians, but also third parties in the face of insurance companies, registries, etc.

Secured and meaningful data is a good opportunity for organizations to save money. The data will be more organized facilitating the processing in order to use it for future budget planning and scientific research.

3. 2. 3. ICT and information security

GDPR is expected to have a significant impact in Information Technology systems, platforms and data architectures that are currently processing personal data (i.e. collecting, managing and storing). This regulation has set out high requirements for data controllers and processors handling personal data including data protection by design and default, recording all processing activities, conducting data protection impact assessment, etc. As such, the need for technology arises. Below are shown main requirements that might demand technology innovation within organizations in order to be GDPR compliant.

3. 2. 4. GDPR impact from technology and information security perspective

GDPR does not only come with challenges and there are great benefits for organizations that are GDPR compliant. They shall be used as a means for achieving business and technology alignment in order to contribute to the organization goals.

Below is shown the impact coming from cybersecurity enhancement and technological improvement as a result of GDPR adoption.

- Better Decision Making and Better Personalized Services for Customers

Data is often the most valuable asset that a company holds and so it is for individuals. With the new regulation, data becomes more consolidated and accurate. Meanwhile, redundant, obsolete, trivial data shall be eliminated. Organizations and customers are clearer on how the data would be used which helps businesses in identification of areas where customer needs are not met and can take much proactive and personalized decisions to increase their customer experience and loyalty.

- Reduced IT Maintenance Costs

As a result of data maintenance and customer consent, IT Maintenance costs are reduced by the retiring of data software and/or applications that are not relevant or compliant. The need to follow GDPR's mandate to keep the data inventory up to date, can reduce the cost of storing data by consolidating information, which might be present in silos or kept in inconsistent formats.

- Innovation

GDPR introduces new concepts related to technology that bring the opportunity not only to innovate within the organizations, but also to build customer trust and confidence through technology improvements. It is expected that new systems will be more sophisticated and embracing the latest technology such as cloud computing and artificial intelligence.

- Cybersecurity within Organization

GDPR is expected to have impact on organizations' cybersecurity policy and practice since it requires companies to take actions in data protection measures to protect consumers' personal data and privacy against data loss or exposure. These activities will help in reduction of attacks and data breaches, as well as better understanding of what is going on across the network.

3. 3. Job creation stimulation by GDPR implementation in specific economic sectors

This Part # 3 of the Report provides an assessment of GDPR implementation impact on job creation in Albania.

This assessment is based on the current available data on business environment and market. In addition, the assessment is also based on the interviews conducted with different businesses in BPO industry as being our mains scope, as well as telecommunication, banking, ICT and healthcare.

3. 3. 1. Impact assessment

Given the wide reaching implications of the GDPR, it is surprising that many companies in Albania may have overlooked the fact that such regulation might even apply to them (i.e. as per article 3 of GDPR). While companies in Europe have implemented already the GDPR, some of the Albanian companies are only at the early stages of GDPR impact assessment associated at this stage.

As a result from interviews the level of awareness on GDPR implementation is at above average compared to the total result. On overall, 40 percent of the interviewees claim to have a high awareness related to the impact of the GDPR implementation on their business operations. In fact, 42.9 percent of the companies interviewed declared to have already taken the proper measures to implement GDPR, while 57.1 percent are lagging behind (please refer to the graph of answers to question No. 8 in Appendix 1).

The high level of awareness on GDPR implications resulted in the BPO industry companies, which are affiliates of international companies offering services to the EU markets. In this case, reaching compliance with GDPR was mainly driven by their suppliers' and contractors constant requirements. Due to this, such BPOs declared to have already implemented GDPR standards in their business processes, thus their knowledge on the GDPR requirements is classified as high. The same applies to other industries working or delivering services to the EU countries. The BPO with ICT services and BPO that offer services only to the Albanian market, classified their knowledge on GDPR as very low, implicating a low readiness to deal with the GDPR implementation requirements.

The responsibility to address issues and compliance with the Albanian Legislation on personal data protection and GDPR based on the interview responses is allocated to the Legal/Compliance Manager by 90 percent of the Companies while other roles such as IT, Human Resources and Administration are involved as a task force on specific issues.

Considering the above observations, it is not surprising that the interviewees claim that increasing their capabilities in terms of knowledge and expertise on GDPR is mandatory with 85.7 percent claiming they need new expertise for

the implementation and post-implementation phases. As a result, 50 percent of the interviewed companies would be prepared to engage a Consulting company to assist them, 78.6 percent would like to train the current staff members while only 21.4 percent are planning to hire new talent to take over the GDPR compliance duties (please refer to the graph of answers to questions No. 6 and 6.1 in Appendix 1). Training of existing staff, is considered as the main approach to fill the gap in expertise and knowledge. The majority of interviewed business (78.6 percent) believe that the training should be outsourced since they do not have in-house expertise on the GDPR. Only 21.4 percent claim to conduct the trainings in-house with the support of their EU based holding company (please refer to the graph of answers to question No. 6.3 in Appendix 1).

Asked whether, in terms of business development and expansion, they have faced any challenges after the GDPR implementation in EU, 42.9 percent responded positively while the rest declared they were not affected so far (please refer to the graph of answers to question No. 9 in Appendix 1). The highest percentage of affected companies fall under the BPO industry, which is analyzed in more detail in the industry based analysis in section 3.3.3. It is very important to highlight that 35.7 percent consider the harmonization of the local law with GDPR requirements as a driving force for expanding and developing further the business in Albania. Nevertheless when asked about future plans in terms of employment of new staff and budgets allocation following the future GDPR implementation, 71.4 percent responded that it is still too early for such an assessment (please refer to the graphs of answers to questions no. 10 and 10.1 in Appendix 1). Most of the interviewed companies are aware of the investments needed in their technology and platforms imposed by compliance requirements of GDPR.

3. 3. 2. Industry-based analysis

BPO Sector

Larger companies operating in the BPO industry, which work extensively with EU based partners and offer services to the EU citizens, declare to be knowledgeable and aware of the GDPR requirements and claim to have already implemented some standards of GDPR as a precondition to continue their business or expand their BPO services. They shared that non-compliance with GDPR requirement in the right time would have had a devastating effect on their business. They explained that the GDPR standards implementation was a requirement imposed by their EU based contractors, who were reluctant to collaborate with companies that were not compliant with GDPR. Fulfilling these requirements has been a challenging process associated with substantial costs in terms of time, effort and investments in their ICT systems modification and adjustments to comply with GDPR.

These companies, due to the lack of implementation expertise, addressed this gap by contracting external consultants with the support of the head offices in cases of affiliated Albanian BPO companies. Such BPOs claim to

have followed a structured approach towards the compliance with GDPR and Albanian legislation on personal data protection. The companies falling in this category mentioned that they would not need to hire new employees, driven by GDPR implementation and compliance efforts, considering that they are in an advanced stage of the process. They have appointed DPOs as per Albanian legislation on personal data protection. In addition, they declared to have followed the approach of teamwork in this domain, allocating the various compliance tasks among their Legal, HR and IT functions (please refer to the graph of answers to question No. 4 in Appendix 1). At the current stage, they claim that the people involved with data protection and GDPR compliance, have been trained accordingly during the implementation phase, and are enrolled in frequent trainings as necessary.

None of the interviewed BPO businesses reported that as the result of the implementation of GDPR standards, the number of their employees has increased. This outcome reinforces the statement that the implementation of GDPR standards as a precondition for doing business with EU based contractors has served primarily the retention of current business performance indicators rather than its expansion in terms of volume or new services.

On the other hand, the BPOs working with EU and Albania, falling under the category of small or medium size enterprises claim that they are aware of the GDPR requirements. However, so far they have not established a well-defined structure to address those. In addition, their current expertise on GDPR and on data privacy in general, is insufficient for the implementation of GDPR. Indeed, these companies have not even finished conducting any internal impact assessments of the GDPR implementation to their business performance and operations, let alone designing actions' plans towards compliance. However, in order to fill this gap they declared they plan to hire external consultants for the implementation phase and for continuous upskilling of their staff members.

In stark contrast to the larger BPOs, this category claims that they have lost business and were urged to limit or stop delivering the services they offered such as digital marketing because they had not taken timely measures to implement GDPR. Thus, it becomes crucial for them to act as soon as possible. They are aware of the new technologies and related costs and this will need extra effort from their side in order to stay in business.

BPO – ICT profile

From the interviews, it resulted that there are significant differences in BPO industry especially with regard to ICT companies compared to those offering BPO services in other industries. The ICT BPO companies are aware of the GDPR, but they rate below the average, in terms of knowledge. None of the interviewed ICT BPO companies has implemented or is planning to implement GDPR. This might be explained from the fact that the ICT BPO services, which are focused on system development, customisation or purely on coding tasks, are not exposed

to personal data, thus might not have been under pressure from their EU based contractors for GDPR compliance. However, these companies might be subject to GDPR as a precondition for BPO business development, in cases they might fulfill system, newly coded or customised platforms, which might require personal data for piloting testing processes. In addition, all the interviewed ICT BPO companies result to lack a structured compliance approach towards the GDPR and Albanian legislation on personal data protection. Based on the conducted interviews, it is implied that there is no formally appointed DPO in most of the interviewed companies. The tasks and responsibilities of the DPO are divided among various functions such as IT, HR or Legal. In some cases outsourced to external providers of such services.

However, some other ICT BPO businesses claim that they have faced some delays or have lost business opportunities because they did not take the measures on time and they lacked necessary local support, because Albania has not harmonised yet the GDPR requirements into its legislation. Three of them reported that these limitations in concluding with new business opportunities were related to specific BPO services that rely extensively on personal data processing such as Digital Marketing, Web Analytics or Online Behavioural Advertising and ICT services, etc.

With the entering into force of GDPR in May 2018, the provision of such services from Albanian BPOs were ceased, or new business opportunities were lost forcing them to find other solutions such as transferring or establishing such a BPO business in EU Member States countries in the Balkans region. Some of the interviewees mentioned that they intend to increase the staff number with 25 percent to 30 percent within this year (please refer to the graph of answers to question No. 10.1 in Appendix 1). Nevertheless, this was not related directly to GDPR implementation, rather with the business expansion of current ITC BPO services. However, they estimate that in case of GDPR adoption into Albanian legislation, they expect a potential growth in terms of business and employment in their area of expertise, because they believe the company reputation will be improved as GDPR compliant ones, improving at the same time their competitive advantage in offering services and doing business with EU based contractors.

In this category as well, filling the gap in GDPR implementation and post-implementation expertise and knowledge, remains a challenge. All of the ICT – BPO businesses assess that they will need to put extra efforts in building their capacities in terms of staff upskilling. They foresee to address this challenge through the support of external consultants in the preparatory phase of GDPR implementation as well as during the course of business in the post implementation phase.

Banking sector

The banking sector has a slightly different approach from the BPO industry. The representatives interviewed are aware and knowledgeable about GDPR

requirements in the above average level. 33.3 percent of the interviewees have already conducted their internal impact assessment and are under implementation process. The drivers that pushed forward the GDPR implementation were business relationships the EU customers. All the banking sector respondents are well aware of the Albanian legislation on personal data protection. In all the cases, there is no DPO appointed as per the GDPR requirements, but they have a DPO, usually Legal or Compliance Manager, who are charged with the formal responsibilities and duties stipulated by Albanian legislation on personal data protection. However, they declared that for specific cases related to data privacy, they share some of the tasks and responsibilities and work closely also with IT, HR and Legal functions.

All the interviewees in the banking sector claimed that they have not experienced any challenges or loss of business opportunities due to the lack of harmonisation of Albanian legislation with GDPR. The interviewees confirmed that in the long term, they plan to hire a DPO responsible, which however, does not imply a meaningful driver for job creation and increase of employment rates.

Only 33.3 percent claim that the people involved with data protection and GDPR compliance, have been trained before commencement of the implementation phase. However, they plan further trainings through external consultants. All the interviewed banks that have not commenced the GDPR implementation actions, declared that they will engage a consulting firm for the implementation phase and for upskilling their current employees.

As declared during the interviews, the banks are relying and expect a supporting and guiding role from the Commissioner in order to take steps that are more measured and plan accordingly.

Telecommunication sector

From the interviews, it is found out that the Telecommunication sector claims to have an above the average level of awareness and knowledge on the requirements, while in terms of the Albanian legislation on personal data protection they consider themselves fully capable and compliant. All the interviewees appear to have a structured approach towards the Albanian legislation on personal data protection, having a DPO in place either Compliance or Legal Manager and a team responsible for specific matters with in IT and /or HR background.

About 66.6 percent of the companies stated that they have taken some preliminary steps for the implementation of GDPR and they are constantly in contact with the Commissioner for further advice and guidance. However, in general they declare that at this phase and with no concrete direction on the GDPR implementation timeline and general indications on its implications, it is early to start with any preparations.

When asked about potential challenges they have faced so far with regard to GDPR, all of the interviewees stated that they have encountered challenges especially with their EU based

contractors. In such cases, telecommunication companies being affiliates of EU international groups, were able to seek advice at the Group DPO or external consultants.

At the current stage, 66.6 percent of the interviewees declared that the people involved with data protection are trained frequently and upskilled with the focus on the local law on Data Protection. However, all of them claim that they plan to engage a consulting firm for the GDPR implementation and to train the employees involved in the process.

Only 33.3 percent mentioned that GDPR implementation in the EU will have a positive impact in terms of expanding business and services. Following to this, they expect to increase the staff number by 3 percent (please refer to the graph of answers to question No. 10.1 in Appendix 1). While 66.6 percent stated they do not expect a business expansion or increase in employment numbers due to GDPR implementation. Rather they stated that it is quite restrictive and they have allocated specific budgets to cover all costs for new technologies and other requirements during the GDPR implementation process.

The consulting service in Albania is a fast growing sector brining a significant impact to the economy. Mainly this sector provides services to local companies but on the recent years, they are reaching to international franchises with offices in Albania. Therefore, the implementation of GDPR will benefit this sector since they are going to be in the forefront of this process by providing consultancy on how to implement and be compliant. If the implementation of GDPR will attract international companies, then consultancy firms are expected to generate an increase in revenue which will be a cause a potential increase in staff demand, especially with experts in cybersecurity and ICT.

Due to the data limitations in Albania, as well as in EU, an exact number of consultancy firms as service providers which will be impacted by GDPR implementation cannot be derived. In addition, as discussed earlier in this report, most of the companies engaged in the survey judge that it is yet early to estimate the impact of GDPR implementation. The only indication available for the Albanian market comes from INSTAT Business Register, implying that in 2018, there were 793 active firms with activities of head offices and management consulting, however it cannot be inferred that these Companies are all able to provide consultancy services related to GDPR implementation and compliance.

3. 3. 3. Conclusions

Albania presents a unique market for GDPR compliance finding itself relatively late in the preparatory process for the GDPR implementation – with many Albanian companies not realizing that GDPR regulation applied to them until only recently. Albanian companies are knowledgeable and claim to posses expertize on the Albanian legislation on personal data protection, however many appear to be unsure of how to approach the GDPR,

and as a result have adopted a “wait and see” approach – choosing to wait for further instructions from the Commissioner before taking action and preparing action plans for GDPR implementation. A relatively underdeveloped risk management culture and comparative lack of experience in managing overseas risks are proving to be serious challenges for many Albanian companies.

At the current state, to avoid non-compliance, the Albanian companies should first analyse the GDPR to identify if it applies to them, and if it does, start analysing their internal data processing activities in order to harmonise them as far as possible with the provisions of the GDPR.

- New opportunities for services and business expansion upon harmonization of the Albanian legislation with GDPR

BPO companies interviewed (83.3 percent) are of the opinion that the GDPR implementation will support them to retain the existing business and it will provide a high potential to expand further the range services in the EU market. However, based on the overall results of the interviews, for the majority of interviewed companies, it is still early to conduct a thorough assessment on the potential job creation and any quantifiable employment growth.

Considering the increasing trend of the BPOs in terms of economy and employment in Albania, it would be advisable to prioritize and draw a detailed action plan for harmonizing the Albanian data protection legislation with GDPR as a matter of high priority; hence providing the BPOs the likelihood to have a competitive advantage, limiting the lost of business opportunities with EU based contractors and boost their expansion in the Albanian market. This would be a benefit for the BPO industry and would be an opportunity for the Albanian market economy and employment growth.

As of the current state, we conclude that companies are planning to upskill the current staff members such as Legal, IT and HR (78.6 percent) in order to take over new responsibilities that respond to the GDPR requirement rather than hire new people (21.4 percent). However, in the long run as the Albanian legislation will be harmonised with GDPR, (35.7 percent) of the Albanian companies interviewed plan to hire at least one DPO (please refer to the graph of answers to questions No. 6.1 and 7 in Appendix 1).

We conclude that the BPO sector in Albania has all the preconditions to flourish given that it will be working in a regulated environment. This is also supported further by the results of our research as stipulated in “General Overview” section admitting “Albania has a large number of graduate students in fields related to BPO services, the strong cultural affinity with some of the EU countries in terms of knowledge of foreign languages and adaptability”.

On the opposite side of the spectrum, the BPOs falling in the small size Companies category, might find it difficult to cope with the adoption of the GDPR. This is expected to be a result

of being relatively weak financially to support the technological change and with no parent company to support them in terms of expertise and investment. Based on the overall assessment and interviews, we expect a negative impact of GDPR implementation for such a category.

All BPOs should start their journey toward GDPR implementation by taking the necessary steps to start an assessment process related to GDPR, which would help them identify and allocate budget for new technologies, staff upskilling and related consulting services.

- GDPR compliance used as a market differentiator from companies

Following to the interviews' results, there is a growing probability that at least some companies will not have started with their GDPR projects, unless there is any formal indication by the Commissioner on the deadline of full completion of GDPR adoption into Albanian legislation. As such, we found that the companies, which have implemented in their business operations and processes the GDPR standards, consider this as a competitive differentiator in the Albanian market.

- Most companies plan to use external consulting firms to accelerate their GDPR preparation

As the GDPR's requirements are deep and complex, preparing for its implementation requires buy-in and support from across the organization and companies have come to an understanding that they do not posses the right expertise to handle the implementation on their own. In response to this, many companies in Albania plan to use external consulting firms to support their preparation actions. This is an opportunity, for the consulting business specialized in personal data protection and GDPR requirements and more specifically in IT and Legal (please refer to the graph of answers to questions No. 6, 6.1 and 6.2 in Appendix 1).

- Cybersecurity professionals

As a result of GDPR, organizations would need to increase their cybersecurity efforts to protect against possible internal and external threats and breaches. Thus, GDPR will further increase the demand for cybersecurity professionals. To address the current skills shortage for cybersecurity professionals, both governments and technology companies will need to invest in more cybersecurity training and education programs.

3. 4. Estimation of the period of implementation of GDPR legislation in practice

In this Part # 4 of the Report is provided a high-level legal analysis of the instrument and legal route of implementation of GDPR in virtue of the law-making process/requirements in place in Albania.

This analysis contains the proposed act for approximation of the national legislation with GDPR provisions and a summary of the procedure that such act would need to go through until its enactment and publication.

In addition, it is provided also a (mere) estimation of the period of implementation of GDPR following the approximation process, taking into consideration, *inter alia*, the rationales that accompany the transitory periods necessary for a reasonable implementation of an enacted act.

3. 4. 1. Approximation instrument and procedure

The Law on Personal Data Protection represents the main instrument that deals with the protection of personal data in Albania. The provisions of this law are like those of Directive 95/46/EC, which has been repealed by GDPR. Hence, although not explicitly mentioned in the body of this instrument, we considered that it is fully aligned with the Directive 95/46/EC.

It is to be emphasized that Albania has started the process of approximation of the national legislation with EU *acquis*, several years ago (i.e. even prior to entry into force of Stabilisation and Association Agreement between Albania and EU). The main instrument used to this purpose and process is that of a law.

In this view, for purpose of approximation of Albanian legislation with GDPR, the Albanian Parliament might enact a law that amends the current Law on Personal Data Protection or a new law that repeals the latter.

The legislative initiative for enacting the specific law according to article 81 of the Albanian Constitution pertains to the Council of Ministers, any member of the parliament, as well as to 20 thousand voters.

Further rules and terms in relation to the route that is pursued by a proposed draft law until its enactment are laid down, *inter alia*, the law no. 9000, dated 301.01.2003 "*On organization and functioning of the Council of Ministers*" as amended ("Law 9000/2003") and the law no. 146/2014, dated 30.10.2014 "*On public consultation*" ("Law 146/2014"), and the sublegal acts issued in application thereto.

For purpose of this section 3.4.1. shall be considered the scenario that relates to the proposal of the draft law by the Council of Minister, which indeed is the largest contributor in this regard (i.e. more than 90 percent of the initiatives pertain to this institution).

The initiative for proposing the approval a project-act (i.e. draft law) might be taken by the prime minister and any minister as per his/her filed of competence. In addition, according to article 26 of the Law 9000/2003, the project-acts that pertain to other central bodies subordinated to the prime minister or the relevant minister shall be submitted for review in the Council of Ministers upon proposal of the prime minister or the relevant minister.

Considering that the personal data protection falls under the authority of the Commissioner (who is appointed by

the Albanian Parliament upon proposal of the Council of Ministers), the latter might submit proposal for the approval of the drat law that intends the approximation of the national legislation with GDPR to the Council of Ministers.

Before being approved by the Council of Ministers and forwarded to the Albanian Parliament, the draft law should undergo the public consultation.

According to the Law 146/2014, any interested party is entitled to submit within 20 working days, from the relevant notification date, its comments and recommendations regarding the draft law. Dependent on the complexity of the project-act, the said term might be extended to 40 working days.

In addition, the project-act, along with the accompanying explanatory report and any other related documentation, shall be submitted, *inter alia*, to the Ministry of Justice (for assessment of the lawfulness, form and content of the project-act), as well as to Ministry for Parliamentary Affairs, Ministry for Europe and Foreign Affairs and Ministry of Finance.

Once the project-act has been approved by the Council of Ministers ("CoM"), it shall be submitted to the Albanian Parliament, where it shall undergo the enactment process through parliamentary commissions and, finally, from the members of parliament.

Article 83 of the Albanian Constitution establishes that draft laws require three voting rounds by the parliament. In the first voting round, the draft law is approved in principle; in the second one, the parliament examines and approves each article of the draft law; and in the third and last voting round, the draft law is approved in its entirety.

Following the parliamentary approval, the President of the Republic of Albania promulgates the law within 20 days after its receipt. Save for exceptional cases, a law enters into force after the elapsing of 15 days following its publication with the Official Gazette of the Republic of Albania.

In the light of the above, the question would be whether there is a need to enact a new law on personal data protection or to amend the current one.

As regards this issue, the practice followed in case of proposal of new law is that the drafting of a new law would be done if the novelties to be introduced would change at least 60 percent of present provisions.

Having said this, we believe that, in case of full approximation with GDPR, such threshold would be met. Hence, the enactment of a new law would be advisable.

3. 4. 2. Proposed transitory period

As mentioned above, the Law on Personal Data Protection has been enacted using as benchmark the provisions of EU Directive 95/46/EC, which has been repealed by GDPR.

As indicated in Table A in section 1.1. of chapter 1 (*Introduction*) of this Report above, the EU Commission has proposed since 2012 the reform of EU legal framework on personal data

protection, which lead to approval of GDPR in 2016.

In addition, the transitory period granted to member states and other stakeholders (i.e. data controllers/processors) for entering into force of the GDPR has been 2 years (article 99). This term appears to have been reasoned (mostly) based on economic and practical arguments that include, *inter alia*, the following:

- Enabling the member states to adopt their national legislations to the provisions of GDPR (i.e. especially in relation to the discretional rooms that it confers onto them).
- Enabling the data controllers/processors to adapt their processing means, rules, policies and mechanisms to the provisions of GDPR (i.e. especially with regard to obligation of information, rights of the data subjects, etc.). Specific attention is granted to the newly established controllers/processors, as well as to the fact that the data controllers/processors that are subject to GDPR should procure for their establishments/affiliates outside EU to be compliant with GDPR.

  In addition, the provisions of the GDPR apply also to data controllers/processor that are not situated in EU, which process personal data as per points (a) and (b) of paragraph 2 of article 3 of GDPR. Hence, the transitory period aims also to raise awareness of all subjects to GDPR to tailor their processing activities in accordance with the provisions thereof.
- The transitional period is considered very important also in relation to the new range of fines introduced by GDPR (i.e. up to 4 % of the total worldwide annual turnover of the preceding financial year of the company or up to EUR 20 000 000; whichever is higher).

In the light of the above, considering the GDPR represents a very substantial and significant material transformation of the EU legislation toward the better protection of personal data protection (i.e. this especially, in relation to the economic and social aspects inherent to the digital era), in case of enactment of a new law that is fully approximated with the material provisions of GDPR, it would be recommendable to include a reasonable transitory period that fits to the complexity and dimensions of the Albanian market.

However, the transitory period provided for under article 99 of GDPR would be deemed too excessive to be replicated to the Albanian market, considering the well-known fact that it is – by far – less complex and significantly smaller than the EU internal market.

Hence, a reasonable transitory period that might be provided for under the provisions of a new law on personal data protection would be a period between 6 months and 1 year, following the publication of this law with the Official Gazette of the Republic of Albania.

3. 5. How GDPR compliance could stimulate development of business consultancy services

In this Part # 5 is outlined the hypothetical impact from GDPR implementation, including challenges and areas for development of business consultancy. The overview is organized to address needs in short-run, during implantation phase, and long-term period, assistance during the post-implementation phase.

With regard to ICT and cybersecurity services, has been identified a wide range of services offered from companies operating in Albanian market in order to help organizations and cover their needs.

Assistance from business consultancy services in the initial implementation phase

As per Statista, in 2018, the average estimated cost for the implementation of the GDPR for UK companies' (FTSE 100) amounted GBP c.160 million.

Before and during the initial implementation phase organizations need to undertake a form of "diagnoses" of the data their managing and their current processing workflow.

This step is important as it address and highlights the risks of the company, which will then flow with an implementation work plan and timeline.

Therefore, the companies in the initial implementation phase would require:

- Action plans to mitigate all risks and assure technical processing of the data in line with GDPR
- Examination of the current process and invest/upgrade of such process in line with GDPR
- Staff training by international or local experts;

Inform/train on the legal part for the GDPR implementation.

GDPR impact on Albanian ICT and information security consultancy services

The GDPR's high requirements for securing personal data brings a new opportunity to consultancy companies that offer their services to guide the affected parties into being GDPR compliant. There are several companies in Albanian market that offer expertise in privacy data protection across organizations and GDPR related services.

Internal audit service providers can help an organization mitigate GDPR compliance risks by identifying ways to improve controls, raising risk awareness and assuring compliance. In addition, since compliance requires continuous focus and effort, internal audit service providers can help in GDPR post-implementation phase.

In the future, companies might have the need to practical guidance during conception of a new or changed

product or service (privacy by design), assessing new and existing systems following the established privacy impact assessment method. Especially, IT companies that provide software development services shall have requests from organizations asking for software development practices and application design and impose greater data security.

3. 6. Assessment of how GDPR can lead to new investments and increased competitiveness

This part # 6 will serve as an overall analysis to assess how the GDPR can contribute to potential new investment.

The potential for new investments is addressed in two ways:

- Local investment – in regards to the need for business consultancy services in dealing with the new regulation to open new opportunities for investments in this sector.
- Foreign investment – concerning the implementation of GDPR to strengthen brand reputation in order to attract new opportunities and investments from EU investors.

GDPR impact on local investment

In order to continue offering products to EU citizens, as well as attract new investments from EU countries, the implementation of GDPR will be a focus.

The biggest challenge especially for SMEs might be the implementation of the GDPR in practice. Compliance with the GDPR requires comprehensive changes to the businesses practice – especially for businesses that do not have in place any kind of privacy procedures before the regulation. Several businesses operating in Albania lack not only data privacy procedures but also knowledge of the new requirements on private data protection and handling. The main costs firms are expected to face in order to be GDPR compliant:

- increased costs of additional data procedures – more value chain functions to be carried out, pseudonymization, documentation, etc.
- investment in new or updated technology and software,
- consultancy services (including IT and legal)
- changes in organizational procedures and structures
- staff training.

According to Christensen *et al*[6], it is estimated that the annual costs for the average SME in the EU, increase by approximately EUR 3,000 – 7,200,

[6] Christensen, Laurits, et al. "The impact of the data protection regulation in the EU." Intertic Policy Paper, Intertic (2013).

depending on the industry, which represents 16 - 40% of annual small and medium-sized enterprise IT budgets.

However, in the long-term, when considering compliance with GDPR as a strategic opportunity for gaining a competitive edge in a data-driven world, companies that target European markets will intensify their efforts by increasing investments in secure data platforms, systems, products and consultancy services on the regulation, as well as training staff members.

With over 2,300 entities in the ICT sector and an increasing labour force with tertiary education, Albania has the potential to support this increased demand of businesses for implementation of the GDPR by offering professional consulting services. The increased demand for GDPR consultancy is expected to expand the market of IT consulting services combined with legal experts. Some of the main services expected be offered in regards to GDPR compliance:

- Assessing the current state of data handling procedures,
- Designing and defining the new procedures,
- Implementing and administering the changes,
- Managing and securing compliance,
- Designing and implementing innovative technologies to solve GDPR concerns.

Start-ups or existing companies expanding in new service lines are expected to require new workforce especially in the ICT sector to aid in implementation of GDPR, thus increasing employment of the sector.

GDPR impact on foreign investment

EU countries count for the highest foreign direct investment (FDI) stock in Albania, with investments mostly in telecommunications and banking sector, both accounting for 29.6% of the total FDI stock in 2018 compared to 33.7% in 2017. The Information and Communication FDIs increased by 1.3%, from EUR 1,170 million in 2017 to EUR 1,185 million in 2018, while Financial services sector FDIs rose from EUR 1,006 million in 2017 to EUR 1,081 million in 2018, or 7.5%.

Out of the top 10 countries with the most FDI stock in Albania, 8 of them are part of the EU. Switzerland counts for the highest foreign direct investment with c. EUR 1,33 million in 2018, followed by Greece with c. EUR 1,22 million FDI stock in Albania, invested mostly in telecommunications and in the banking sector as the two largest telecommunication companies in the country consist of the Greek capital. The Netherlands ranks third by foreign investment stock followed by Canada, Italy, Turkey, and Austria.

As most FDI flow in Albania comes from EU countries, GDPR compliance is important in expanding and attracting new investment opportunities in the country. Albania attracts foreign investments mainly due to:

- low labour costs,
- low rents,
- fiscal incentives,

- young workforce,
- strategic geographic location.

The European Union is limiting the export of data to organizations in countries that do not have adequate privacy protections. As a result, Albanian businesses that want to import personal data from Europe face the prospect of either lost business opportunities or increased costs to provide data privacy protection. The exact value of the potential losses is not clear, but the strong objection to the privacy standards from part of the business community suggests that the costs are large (based on Econsultancy research, 41.9% of surveyed business in the EMEA region responded noncompliance with GDPR would cause revenue loss).

Since many Albanian companies rely on both EU and non-EU customers, it would be easier for the whole company to become GDPR compliant than to apply additional data security measures only to the data of EU citizens.

However, the adoption of GDPR has recently been a strict requirement for companies dealing with outside the border transactions and for outsourcing services. Complying with GDPR privacy protections is expected to raise business costs of data protection, however, in the long term it could expand international business opportunities of investment in Albania and reduce business costs. The adoption of the new regulation is expected to strengthen the reputation of Albania in the eyes of European and international investors, (based on Econsultancy data, 50.2% of businesses in EMEA region have responded non-compliance can cause reputational damage). Moreover, considering training and advancement in capability on GDPR compliance procedures, foreign companies operating in business consultancy services could see Albania as a strategic market to expand or outsource their businesses.