ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΜΕΤΑΠΤΥΧΙΑΚΟ ΣΤΑ
ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ
MSc IN **INFORMATION SYSTEMS**

M.Sc. THESIS:

Data Protection Impact Assessment on GDPR

ΝΙΚΟΣ ΚΡΙΣΙΛΙΑΣ
M316001

ΛΙΛΙΑΝ ΜΗΤΡΟΥ
ΥΠΕΥΘΥΝΗ ΚΑΘΗΓΗΤΡΙΑ

Αθήνα, Ιούνιος 2018

Table of Contents

0. Indexes and Acknowledgments

0.1. Figure Index

0.2. Table Index

0.3. Keywords & Acronyms

- Data Protection Impact Assessment: **DPIA**
- Personal Identifiable Information: **PII**
- Internet of Things: **IoT**
- Privacy-Enhancing Technologies: **PETs**
- Information and Communications Technologies: **ICT**
- Trusted Third Party: **TTP**
- Supervisory Authorities: **SAs**
- Data Protection Officer: **DPO**
- General Data Protection Regulation: **GDPR**
- Data Protection Directive (95/46/EC): **DPD**
- European Union: **EU**
- Information Technology: **IT**

0.4. Abstract

The main purpose of this essay is to initially explain and mention the main points of the General Data Protection Regulation (GDPR) and to mainly focus upon the Data protection Impact Assessment (DPIA) procedure. It mainly focuses on the importance of conducting DPIAs not only for the compliance with the GDPR's provisions but also for the protection of rights and freedoms of data subjects.

Furthermore, a detailed description of the steps for conducting DPIAs is presented along with DPIA's challenges and difficulties.

1. Introduction to GDPR

In May this year, Europe's data protection legal framework underwent its biggest change. Since it was adopted in the middle 90s, the amount of digital information we create, capture, and store has vastly increased. Simply put, the old regime was no longer fit for purpose. The solution is the European General Data Protection Regulation (GDPR, 2016/679), which came into force on May 25 2018.

The GDPR will change how businesses and public sector organisations have to handle the information of customers and it will harmonize data protection laws across Europe. The GDPR is Europe's new framework for data protection laws, which replaces the previous 1995 data protection directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data within the European Union). Until 25/5/2018, each member state in the EU operated under the current 1995 data protection regulation and had its own national laws, which transposed the European Framework. For example, the Greek National Law 2472/1997 incorporates the main choices of 95/46/EC Directive and enforces its fundamental principles [38].

Although respectable at the time of its introduction, it lacked uniformity of data subjects' rights across the EU and did not provide legal protection from inadequate personal data processing outside of EU. A difference in levels of protection derived from the existence of differences in the implementation and application of Directive 95/46/EC. In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. The GDPR provides a margin of maneuver for Member States to specify its rules, including the circumstances for specific processing situations (i.e. determining more precisely the conditions under which the processing of personal data is lawful) [37].

Directive 95/46/EC provided a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not, in all cases contribute, to improving the protection of personal data. Such indiscriminate general notification obligations should

therefore be abolished, and replaced by effective procedures and mechanisms which focus instead, on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes [37].

0.1. What did the law require until 25/5/2018

Data Protection Directive 95/46

The Data Protection Directive 95/46/EC generally sets out direct statutory obligations for controllers, but not for processors (we will define these terms later in this section). Processors are generally only subject to the obligations that the controller imposes on them by contract. By way of example, in a service provision scenario, say a cloud hosting service, the customer will typically be a controller and the service provider will be a processor.

Furthermore, at present the national data protection law of one or more EU Member States applies if [39]:

- the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. When the same controller is established on the territory of several Member States, each of these establishments should comply with the obligations laid down by the applicable national law (Article 4(1)(a)); or

- the controller is not established on EU territory and, for purposes of processing personal data makes use of equipment situated on the territory of a Member State (unless such equipment is used only for purposes of transit through the EU) (Article 4(1)(c)); or

- the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law (Article 4(1)(b)). Article 4(1)(b) has little practical significance in the commercial and business contexts and is therefore not further examined here. The GDPR sets out a similar rule.

Conclusively, some of the Directive's subjective and controversial issues that we mentioned led to the need of enhancing the legal framework regarding the processing of personal data, through the GDPR enforcement.

0.2. The importance of GDPR

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU). The new GDPR is an evolution of the EU's existing data rules, the Data Protection Directive (DPD). While co-opting most (but not all) provisions from the 1995 Directive, GDPR remedies the Directive's shortcomings by extending its scope of application. It intensifies existing requirements and introduces several new ones for legal entities, in addition to multiplying the adverse effects for noncompliance and negligence. The regulation is designed to "harmonise" data privacy laws across Europe as well as give greater protection and rights to individuals.

After more than four years of discussion and negotiation, GDPR was adopted by both the European Parliament and the European Council. Although the Regulation has been designated since 27th of April 2016 it will come into effect in 25th of May 2018. The two year preparation period has given businesses and public bodies, covered by the regulation, the time to prepare for these changes.

There are updated rights for people to access the information companies hold about them, obligations for better data management for businesses, and a new regime of fines. Individuals, organisations, and companies that are either 'controllers' or 'processors' (we will analyze later these terms) of personal data will be covered by the GDPR. It's a regulation that is relevant to every organisation, irrespective of size or sector. Accountability is set at the heart of the Regulation and no one can ignore it. The territorial scope spreads outside of the European Union and affect every transaction of data concerning European personal data. GDPR will harmonize the EU data privacy law landscape. In the next paragraph we analyze the most significant elements of the new regulation, some of which are brand new while others remediate the Directive's shortcomings.

0.3. The key points of the GDPR

Before we proceed to the key points of the GDPR we must first define the basic terms and definitions in order to fully comprehend this thesis. Article 4 of GDPR presents the key definitions as follows [37]:

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

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

'profiling' *means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*

'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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*

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

'third party' *means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;*

'personal data breach' *means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*

'supervisory authority' *means an independent public authority which is established by a Member State pursuant to Article 51*

'cross-border processing' *means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

Fig. 1 GDPR

In the full text of the GDPR there are 99 articles and 173 recitals setting out the rights of individuals and obligations placed on organisations covered by the regulation.

GDPR Key Points	
Broader definition of ''personal data''	**Privacy by Design and by Default**
Lawful basis for processing	**Data Protection Impact Assessment**
New Data Subject Rights	**Penalties**
Data Protection Officer	**Data Breach Notification**
Accountability	**Non-EU territorial effect**
Data mapping	

Tab. 1 GDPR Key Points

Broader definition of ''personal data''

Both personal data and sensitive personal data are covered by the GDPR. Personal data, a complex category of information, broadly means a piece of information that can be used to identify a person. As stated above, personal data is any information that relates to an identified or identifiable living individual. Additionally, different pieces of information, which collected together can lead to the identification of a particular

person, also constitute personal data. The GDPR makes clear that the concept of personal data includes online identifiers and location data (recital 30 and 64 of the regulation) – meaning that the legal definition of personal data now puts beyond any doubt that IP addresses, mobile device IDs, geolocation data are all personal and must be protected accordingly. This means that these types of data will now be subject to fairness, lawfulness, security, data export and other data protection requirements just like every other type of 'ordinary' personal data.

Sensitive personal data encompasses genetic data, information about religious and political views, sexual orientation, and more. These definitions are largely the same as those within current data protection laws. It will be very useful to mention the special categories of personal data (sensitive personal data) as stated by the GDPR's Article 9 [37]:

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."

It is also mentionable that GDPR distinguishes the personal data relating to criminal convictions and offences (Article 10) from the special categories of personal data and the processing of the former data are prohibited unless the criteria mentioned in Article 10 apply.

Lawful basis for processing

The requirement to have a lawful basis in order to process personal data is not new. It replaces and mirrors the previous requirement to satisfy one of the 'conditions for processing' under the DPD. However, the GDPR places more emphasis on being accountable for and transparent about the lawful basis for processing. The six lawful bases for processing are broadly similar to the old conditions for processing, although there are some differences. Every organization needs to review its existing processing, identify the most appropriate lawful basis, and check that it applies. In many cases it is likely to be the same as its existing condition for processing.

Public authorities need to consider the 'public task' basis first for most of their processing, and have more limited scope to rely on consent or legitimate interests. The

GDPR also brings in new accountability and transparency requirements. Every organisation should therefore make sure, it clearly documents its lawful basis so that it can demonstrate its compliance in line with Articles 5(2) and 24.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever an organisation processes personal data [37]:

Lawful base	Description
Consent	the data subject has given consent to the processing of his or her personal data for one or more specific purposes
Contract	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
Legal obligation	processing is necessary for compliance with a legal obligation to which the controller is subject
Vital interests	processing is necessary in order to protect the vital interests of the data subject or of another natural person
Public task	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
Legitimate interests	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

Tab. 2 Lawful bases

From these lawful bases, the most unclear and confusing is the "legitimate interest" because there can be a vast variety of opinions upon this matter, depending on many organizational factors. There is a misconception that legitimate interest allows marketing uses of personal data without user consent. While the "legitimate interest" consist an exception, it is always weighed against personal data rights. For example, a company could utilize data without consent under legitimate interest if it were under court order to do so, or if the data were needed to protect some vital interest like human

rights. But otherwise, consent is needed, and it's not enough that a user has agreed to receive marketing info.

Privacy by Design and by Default

In choosing to include privacy by design and privacy by default as key principles in the GDPR, the legislator has acknowledged that privacy cannot be ensured only by means of legislation, but that it should be a fundamental component in the design and maintenance of information systems, by placing technical and organizational controls and measures in order to achieve this. Additionally, the GDPR for the first time addresses data protection by design as a legal obligation for data controllers and processors, making an explicit reference to data minimization and the possible use of pseudonymisation. On top of this, it introduces the obligation of data protection by default, going a step further into stipulating the protection of personal data as a default property of systems and services, which means that the strictest settings about privacy must be initially implemented without the user's involvement [40].

Accountability

GDPR includes a direct reference to the "accountability principle" in Article 5 par. 2 and Article 24, which requires the implementation by controllers of appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR, and review and update those measures where necessary through notably internal and external assessments such as certifications and privacy seals. What measures will be appropriate in each case, will depend on the nature, scope, context and purposes of the relevant processing as well as the risks for rights and freedoms of individuals.

The notion of accountability is not new to privacy law and policy. It was formally introduced into data protection regulation in 1980 when it was explicitly included as a basic data protection principle in the Organisation for Economic Co-operation and Development (O.E.C.D.) Guidelines. Since then, the accountability principle has been included in a variety of international data protection instruments as one of several core

principles and is slowly (but surely) finding its way into national data protection laws. While accountability used to be all about allocating responsibility for privacy compliance, it is now about requiring a proactive, systematic and ongoing approach to data protection and privacy compliance through the implementation of appropriate data protection measures (It helps in moving data protection from theory to practice). Accountability goes beyond compliance with the rules as it implies culture change. Various international data protection instruments are being revised to reflect that change.

Needless to say that this obligation is very vague and many controllers will rightfully wonder what measures they would be expected to implement. The GDPR itself provides very little guidance in this regard. Implementing privacy policies alone, will certainly not achieve compliance with the accountability obligation. Rather, controllers will be required to implement a range of measures as needed to ensure compliance with all of their obligations under the GDPR. In addition, they must implement measures enabling them to objectively demonstrate such compliance. This requirement will need close consideration in practice. Controllers will need to thoroughly document their data protection efforts and, if requested, make such documentation available to authorities. Any data protection measures implemented will also need to be periodically reviewed and updated as appropriate.

Article 24 par. 3, supplemented by Recital 77, provides that adherence to approved codes of conduct and certification mechanisms may help demonstrate compliance with the accountability obligation. Hence, controllers can expect codes of conducts and certification mechanisms to specify the measures required in order to comply with their accountability obligations. Further guidance on the implementation of appropriate measures and the demonstration of compliance, including on how to identify, assess and mitigate risks associated with data processing, can also be expected from the EDPB.

The accountability provision is qualified by the so-called risk-based approach. The more likely and severe the risks from the proposed processing, the more measures will be required to counteract those risks. According to Recital 75, processing which could lead to physical, material, or non-material damage would be particularly likely to

constitute 'risky' processing requiring particular attention. Recital 75 further provides the following examples as potentially risky processing:

- processing that may give rise to discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage,
- processing that might deprive data subjects of their rights and freedoms or prevent them from exercising control over their personal data,
- processing of sensitive personal data or data relating to criminal convictions or offences,
- processing for purposes of profiling,
- processing of personal data of vulnerable natural persons, in particular of children and
- processing involving a large amount of personal data and affecting a large number of data subjects.

Complying with the GDPR accountability provision is a complex task. The very basic Article 24 does not do justice to the overarching concept of accountability which essentially requires controllers to perform all of their data processing operations in compliance with the GDPR and to be able to objectively demonstrate such compliance. A best-practice approach for organisations would be to build and implement a comprehensive privacy management program. In a nutshell, this would include implementing:

1. Establish transparent internal data protection and privacy policies. These need to be approved and actively endorsed by the highest level of the organisation's management.
2. Put in place appropriate and effective internal processes and tools to implement these policies. This ensures that data protection principles and obligations are complied with and that individuals are adequately protected from risks stemming from the processing of their personal data.
3. Inform and train all people in the organisation on how to implement these policies.

4. Implement various adequate controls to ensure compliance with the various GDPR requirements (such as personal data inventories/ records of processing activities, tailored privacy policies and notices, data breach handling procedures, security and retention policies, privacy enhancing measures by implementing data protection by design or by default when building new products or services, conducting data protection impact assessments when the processing is likely to result in a high risk, processes for selecting and managing data processors, etc).
5. Monitor and assess the effectiveness of this implementation. Out of this monitoring and measuring, the organisation needs to be able to demonstrate to external stakeholders and supervisory authorities the quality of the implementation.

Data Protection Impact Assessment (Article 35)

Data protection impact assessments (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

The GDPR mandates that a DPIA must be conducted where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". The three primary conditions identified in the GDPR are:

- A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.
- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences.
- Systematic monitoring of a publicly accessible area on a large scale.

The outcome of a DPIA is a set of actions that the organization should perform in order to mitigate the potential impact to the rights and freedoms of data subjects.

Data Subject Rights

Privacy Notice (Articles 13 & 14)

Privacy notices are not new but under the GDPR privacy notices can no longer be generic and must be specific for every purpose of processing activity and must follow the requirements as stated below:

- the identity and the contact details of the controller
- the contact details of the data protection officer
- the purposes and legal basis for the processing
- where the processing is based on legitimate interests, details of what these are
- the recipients or categories of recipients of the personal data
- details of any transfer to a third country and details of the safeguards and the means by which to obtain a copy of them or where they have been made available
- the retention periods or the criteria used to determine that period
- details on rights of access to and rectification/deletion of personal data. Rights to object to processing and the right to data portability
- if processing is based on consent, the right to withdraw consent
- the right to lodge a complaint with the supervisory authority
- details on whether the data subject is obliged to provide the personal data and the consequences of failure to provide it
- details of any automated decision making, including details of the logic used and potential consequences for the individual

Right of access (Article 15)

An individual has continuing rights under the GDPR to establish whether a controller processes information relating to him/ her, and to access and obtain a copy of that data and certain additional information in relation to the processing, such as its purposes, the categories of data, the recipients of the data, and the existence of additional rights such as the rights to erasure and objection. As is the case currently, the exercise by an

individual of his/ her access rights cannot prejudice the rights and freedoms of other individuals, and the right of access is not an absolute right.

Right to rectification (Article 16)

When personal data are inaccurate, data subjects have the right to have incomplete personal data completed without undue delay from the controller.

Right to erasure or right to be forgotten (Articles 17)

The right to have personal data rectified, blocked or erased already exists under existing data protection rules. However, enforcing those rights involves a relatively high threshold for individuals, and requires a demonstration that the data controller has contravened data protection principles. Partly as a result of the Google Spain decision of the Court of Justice of the European Union, however, there has been much more emphasis on the right of erasure or "the right to be forgotten", and this focus is reflected in the provisions of the GDPR.

Under the GDPR, every individual has the right to have his/ her data erased, or the "right to be forgotten", in circumstances where:

- the data is no longer necessary for the purpose for which they were collected;
- processing is based on consent, but the individual has withdrawn consent and there is no other legal ground for continued processing available to the controller;
- an individual has exercised his / her right to object, and there is no overriding legitimate interest on which the controller can continue to legitimise its processing;
- the data is unlawfully processed;
- the erasure is required by a law applicable to the controller; or
- the data was collected in connection with the offer of information society services to a child.

Taking account of available technology and the cost of implementation, the controller is required to take reasonable steps, including technical means, to inform other controllers processing the data that the individual has requested erasure of links to, or copies or replication of, the data. The right, however, is not an absolute right, and

a controller will be in a position to continue processing the data on the basis of freedom of expression and information, where the controller is required to comply with the legal obligation which requires processing (bearing in mind that this has to arise under EU or member state laws), or if the processing is required to establish, exercise or defend legal claims.

The data subject right to restriction of processing (Article 18)

Individuals have the right to require that a controller restricts its processing of his/ her data in some circumstances, including where the data is inaccurate (for the period during which the controller is verifying the data). The data is no longer required in light of the purposes of the processing but the individual requires the data in connection with legal claims, or the data subject has exercised his/ her right to object (pending verification of any legitimate grounds of the controller which override those of the data subject).

Right to Portability (Article 20)

The right to data portability is a new right introduced by the GDPR, and allows individuals to obtain and, importantly, reuse their personal data. A data subject can either obtain the data for himself/ herself and, in turn, provide it to a third party (if he/ she so wishes), or require the data controller to transfer the personal data directly to a third party.

Right to object (Article 21)

As with the right to be forgotten, an individual has the right to object to the processing for specified purposes or in a specified manner on the ground that, for specified reasons, it causes or is likely to cause unwarranted substantial damage or distress. Under the GDPR, the existing right to object to processing continues, along with some clarifications and expansion. As is currently the case, any individual has the right to object to direct marketing at any time, and in that event, the controller must stop using the information for marketing purposes.

However, an individual can also object where:

- retaining the data is no longer necessary for the purposes for which they were collected,
- consent has been withdrawn and there is no other legitimate ground for processing,
- processing is based on a public interest or a legitimate interest of the controller, in which case, unless there are overriding legitimate interests, the controller must cease the processing. In this regard, there is no longer any reference to their being "unwarranted substantial damage or distress to the data subject", and instead, controllers must take into account "grounds relating to the data subjects particular situation", which is a broader concept,
- the data has been unlawfully processed,
- erasure is required under a legal obligation to which the controller is subject under EU or member state law or
- the data was collected in the context of the provision of information society services to a child.

The Right not to be subject to automated decision making and profiling (Article 22)

There is an existing right not to be subjected to processing which is wholly automated and which produces legal effects or otherwise which significantly affects an individual, and which is intended to evaluate certain personal matters, such as creditworthiness or performance at work, unless one of a limited number of exemptions applies. Under the GDPR, individuals will continue to have the right not to be subject to decisions based solely on automated processing in a similar manner, with additional restrictions applying in relation to automated processing of special categories of data. Interestingly, the GDPR specifically references profiling, which is defined as "any form of automated process to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements". The exceptions to automated decision making are more narrowly drawn than under current rules. Whereas previously, such processing was permitted in the course of considering whether to enter into a contract, or with a view to entering into a

contract or for the performance of a contract, under the GDPR, automated processing will only be permitted, in the context of contract, where it is a "contractual necessity".

Penalties

There has been a lot of focus on the substantially large fines that come with the General Data Protection Regulation for non-compliance. A fine of €20 million or 4% of annual turnover will be a significant amount for any company to have to pay. It is important to note that these figures are the maximum figures. Supervisory authorities will have the scope to impose fines of a lower amount, or take a range of actions such as [37]:

- Issue warnings
- Issue reprimands
- Order compliance with Data Subject requests
- Communicate the Personal Data breach directly to the Data Subject

Article 83 of the General Data Protection Regulation provides details of the administrative fines. There are two tiers of fines. The first is up to €10 million or 2% of annual global turnover of the previous year, whichever is higher. The second is up to €20 million or 4% of annual turnover of the previous year, whichever is higher. Generally speaking, breaches of controller or processor obligations will be fined within the first tier, and breaches of data subjects' rights and freedoms will result in the higher level fine.

The value of the fine to be imposed is not clear-cut and the behaviour of the organisation will be taken into account when determining the value of the fine. This means that organisations certainly have the opportunity to influence the reduction of any fines by acting to fully comply with the Regulation. This includes promoting a culture of data protection and being able to show the steps taken to comply. Organisations that proactively report breaches will be given more credit, showing that the intention and attitude of a company will be considered.

Data Protection Officer

DPOs are responsible for educating the company and its employees on important compliance requirements, training staff involved in data processing, and conducting regular security audits. DPOs also serve as the point of contact between the company and any Supervisory Authorities (SAs) that oversee activities related to data. As outlined in the GDPR Article 39, the DPO's responsibilities include, but are not limited to, the following:

- Educating the company and employees on important compliance requirements
- Training staff involved in data processing
- Conducting audits to ensure compliance and address potential issues proactively
- Serving as the point of contact between the company and GDPR Supervisory Authorities
- Monitoring performance and providing advice on the impact of data protection efforts
- Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
- Interfacing with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information

DPOs may be a controller or processor's staff member and related organizations may utilize the same individual to oversee data protection collectively, as long as it's possible for all data protection activities to be managed by the same individual and the DPO is easily accessible by anyone from any of the related organizations whenever needed. It is required that the DPO's information is published publicly and provided to all regulatory oversight agencies.

Data Breach Notification

Data controllers are required to report a personal data breach to the competent Supervisory Authority (SA) without undue delay and, where feasible, not later than 72 hours after becoming aware of it unless the personal data breach is unlikely to result in

a risk to the rights and freedoms of data subjects. If a notification is made after the 72 hour period has expired, the data controller must explain the reasons for the delay. The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned,
- the name and contact details of the relevant Data Protection Officer or contact point,
- the likely consequences of the data breach and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.
- Communication of a personal data breach to the data subject (Article 34)

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the controller must communicate the breach to the data subject without undue delay. The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Officer or contact point,
- the likely consequences of the data breach and
- measures taken or proposed by the controller to address the breach and/ or mitigate its effects.

Non-EU territorial effect

There is a common misconception which states that the GDPR applies only in the European Union area. However, this is not the case because there can be circumstances, described below, where its territorial scope can be extended. The territorial scope of the GDPR can be extended when:

- data controllers and processors are located in the EU, whether or not the processing takes place in the EU;

- data controllers and processors are located anywhere in the world, for the processing of personal data of subject located within the EU for the activities of offering goods or services, or monitoring behaviour taking place in the EU;
- a Member State national law is applicable to the case. Consequently, all providers of goods and services with a customer base in the EU or any website or mobile application that utilizes mechanisms of online behavioral advertising shall be subject to the GDPR.

Data mapping (Article 30)

Data Mapping is the process of identifying, understanding and mapping out the data flows of an organisation. A good Data Map (also referred to as a "Data Inventory") will provide a comprehensive overview of the data flows within, to and from an organisation. For example, a Data Map will illustrate:

- the various categories of data held and processed by individual business units,
- data transfers and disclosures between different business units and to third parties, such as service providers. In general, data mapping requires comprehensive information gathering from all business units globally, and visualisation of the information gathered

Additionally the data map answers to below questions described by the Figure 5:

Fig. 2 Data Mapping

More specifically Article 30 of GDPR "*Records of processing activities*", along with the requirements of the register that the controller and the processor must maintain (par. 1 and 2) it clearly states that the register:

- should be in writing and electronic form (par. 3),
- should be available to the supervisory authority on request (par. 4) and
- "*The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."*

The information gathering process should not be a stagnant exercise, rather it should be a dynamic consultation with the objective of gaining a comprehensive understanding of various business functions and activities in order to produce a meaningful and truthful Data Map [41].

Understanding one's data flows is an essential prerequisite for any privacy compliance strategy. Without understanding what data are collected and processed and where that data flows to and from, it is impossible to ensure that the data processing activities are compliant with applicable privacy laws and regulations. For example, it would not be possible to ensure compliance with cross-border data transfer rules without knowing which types of data are disclosed to which recipients in which countries. From a GDPR perspective, Data Mapping will assist controllers (and, in some instances, processors) to become compliant with various new privacy requirements as they apply to them, including:

- the requirement to maintain detailed records of an organisation's data processing activities and to make these records available to supervisory authorities on request,
- the accountability requirement according to which controllers must ensure and be able to demonstrate that their processing activities are performed in compliance with the GDPR and
- the data protection by design and by default requirements.

2. Privacy in the digital age

Before proceeding, it is an absolute necessity to comprehend that one of the most fundamental right in the human history is the right to privacy. Privacy and data protection constitute the main core values of individuals and of democratic societies nowadays. This has been acknowledged not only by the European Convention on Human Rights [24] but also from the Universal Declaration of Human Rights [25] that enshrine privacy as a fundamental right. Furthermore, Article 8 of the European Convention on Human Rights, provides a right to respect for one's "private and family life, his home and his correspondence". Similarly to that, the Charter of Fundamental Rights of the European Union defines the "respect for private and family life" (Article 7) and adds a very specific article on "protection of personal data" (Article 8). Moreover, on an even wider scope, Article 12 of the Universal Declaration of Human Rights protects an individual from "arbitrary interference with his privacy, family, home or correspondence," and "attacks upon his honor and reputation". It needs to be said that privacy protection is not only to be regarded as an individual value, but also, maybe even more importantly, as an essential element in the functioning of democratic societies because the respect and the protection of privacy is the cornerstone of people's dignity and free will.

It is a fact that during the last decades we have experienced an information and technological revolution. Consequently, as time passes by, the development of the existing technology, as well as the appearance of new technological achievements, such as biometrics, cloud computing, smart devices, or the Internet of Things, has led to the exchange of a huge flow of data both in the public and in the private sectors (we will analyze this to a separate section later). Especially in the last 20 years, the concept of everyday life has dramatically changed. The way people do their shopping, the way payments are made, or even the way that social life is organized implies the storage and the use of a massive amount of data. Nowadays, digital technology enables the preservation of the minutia of everyday moves of the citizens, of their likes and dislikes, of their habits and interests and of who they are and what they own. [26] Online purchases, payments with credit cards, digital IDs, surveillance cameras installed in cities, and the use of smart phones which enable users to post information on different social media about their location and activities are only some of the circumstances of

modern life which give rise to privacy concerns. Our freedom of expression and our liberty are threatened by the surveillance of our internet usage, thought patterns and intentions that can be extrapolated from our website visits (rightly or wrongly), and the knowledge that we are being surveilled can make us less likely to research a particular topic. We lose our perspective, and our thoughts can be pushed in one direction as a result. Similarly, when things we write online, or our private communications with others, are surveilled, and our self-censor as a result, we lose our spontaneity, and the development of further ideas is stifled [27]. George Orwell, in his novel "1984", was one of the first who tried to explain the importance of privacy, by using the Big Brother's metaphor, in the context of a totalitarian society. This extreme example, but not an impossible one, shows the ultimate negative effect of the control of citizen's personal data by a totalitarian regime. However, apart from this scenario, numerous privacy concerns arise in the context of daily activities in the transaction and relations in between citizens and/or companies [28].

To summarize, now more than ever, privacy consist an absolute necessity and it is the most important and crucial factor in protecting the privacy and freedom of every individual.

2.1. Benefits of Privacy

Very often courts and commentators struggle to articulate why privacy is valuable. They see privacy violations as often slight annoyances. At this section we will try to explore the benefits of privacy and why privacy matters a lot. Here are some reasons why privacy matters: [29]

Limit on Power

Privacy is a limit on government power, as well as the power of private sector companies. The more someone knows about us, the more power they can have over us.

Respect for Individuals

Privacy is about respecting individuals. If a person has a reasonable desire to keep something private, it is disrespectful and unacceptable to ignore that person's wishes without a compelling reason to do so.

Reputation Management

Privacy enables people to manage their reputations. How we are judged by others affects our opportunities, friendships, and overall well-being. Although we can't have complete control over our reputations, we must have some ability to protect our reputations from being unfairly harmed.

Maintaining Appropriate Social Boundaries

People establish boundaries from others in society. These boundaries are both physical and informational. We need places of solitude to retreat to, places where we are free of the gaze of others in order to relax and feel at ease. If we live in a constant environment of exposure we won't be able to express ourselves and truly relax.

Trust

In relationships, whether personal, professional, governmental, or commercial, we depend upon trusting the other party. Breaches of confidentiality are breaches of that trust. In professional relationships such as our relationships with doctors and lawyers, this trust is key to maintaining candor in the relationship.

Control Over One's Life

Personal data is essential to so many decisions made about us, from whether we get a loan, a license or a job to our personal and professional reputations. Personal data is used to determine whether we are investigated by the government, or searched at the airport, or denied the ability to fly. Indeed, personal data affects nearly everything, including what messages and content we see on the Internet. Without having knowledge of what data is being used, how it is being used, the ability to correct and amend it, we are virtually helpless in today's world.

Freedom of Thought and Speech

Privacy is key to freedom of thought. A watchful eye over everything we read or watch can chill us from exploring ideas outside the mainstream. Privacy is also key to protecting speaking unpopular messages. And privacy doesn't just protect fringe activities. We may want to criticize people we know to others yet not share that criticism with the world. A person might want to explore ideas that their family or friends or colleagues dislike.

Freedom of Social and Political Activities

Privacy helps protect our ability to associate with other people and engage in political activity. A key component of freedom of political association is the ability to do so with privacy if one chooses. We protect privacy at the ballot because of the concern that failing to do so would chill people's voting their true conscience. Privacy of the associations and activities that lead up to going to the voting booth matters as well, because this is how we form and discuss our political beliefs. The watchful eye can disrupt and unduly influence these activities.

2.2. Technologies that led to an increase in the spread of personal data

Data creation is occurring at a record rate. [30] In 2010, the world generated over 1 zetabytes (ZB) of data; in 2014, generated 7 ZB a year and by 2020 we will generate nearly 45 ZB. In order to put this into perspective, 20 petabytes of capacity was the world's production of hard-disk drives in 1995 [31] and 1 zetabyte equals 50 thousand times this capacity. Paula Doe states at her article [32] that by 2020 the average internet user will be transferring 1.5 GB of digital data per day and future autonomous vehicles might be transferring 4TB of digital data per day. Moreover, data production will be 44 times greater in 2020 than in 2009 [33] and the volume of data worldwide is expected to double every 1.2 years [34].

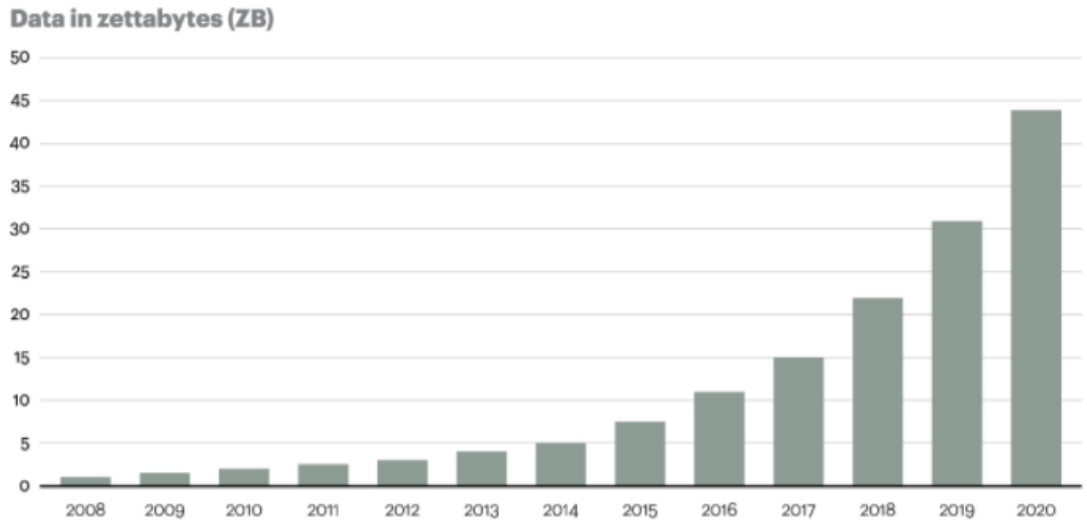

Fig. 3 *Data growth 2008 – 2020 (1)*

Much of this data explosion is the result of the development of **Internet of Things (IoT)** which led to a dramatic increase in devices located at the periphery of the

network including embedded sensors, smartphones, and tablet computers. The analyst firm Gartner says that by 2020 there will be over 26 billion connected devices. [35]

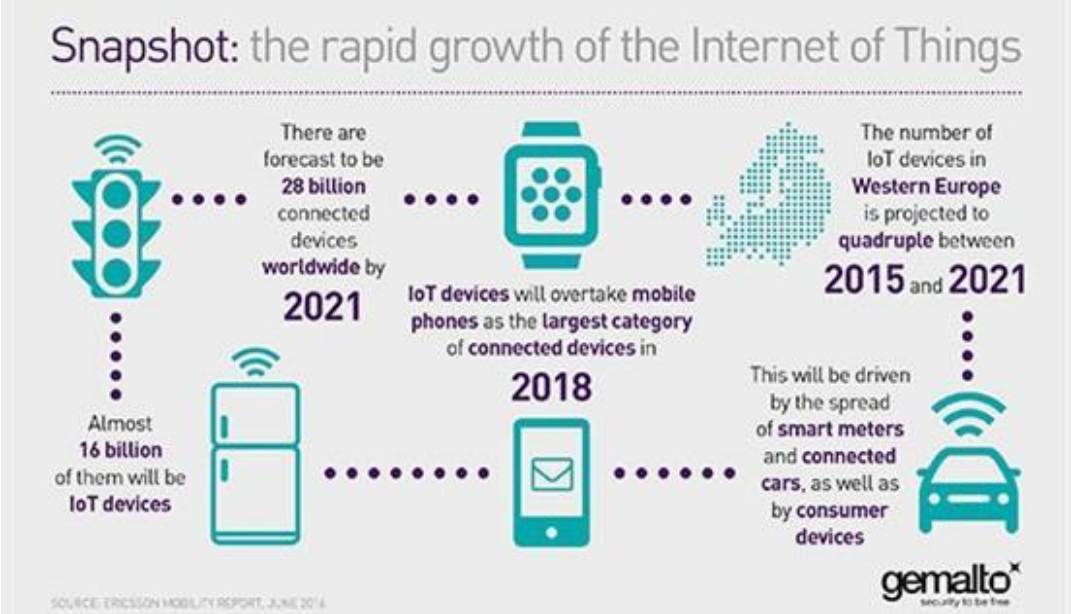

Fig. 4 *The growth of IoT (2)*

That's a lot of connections (some even estimate this number to be much higher, over 100 billion). The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things.

Furthermore, this data explosion was increased by the development of **Cloud Computing**, which is the delivery of computing services - servers, storage, databases, networking, software, analytics and more - over the Internet ("the Cloud"). A more strict definition of the term cloud would be: "*A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers*." [36] but the main point is that cloud computing made the storage of information a very easy task because it transferred the physical storage space at a remote location.

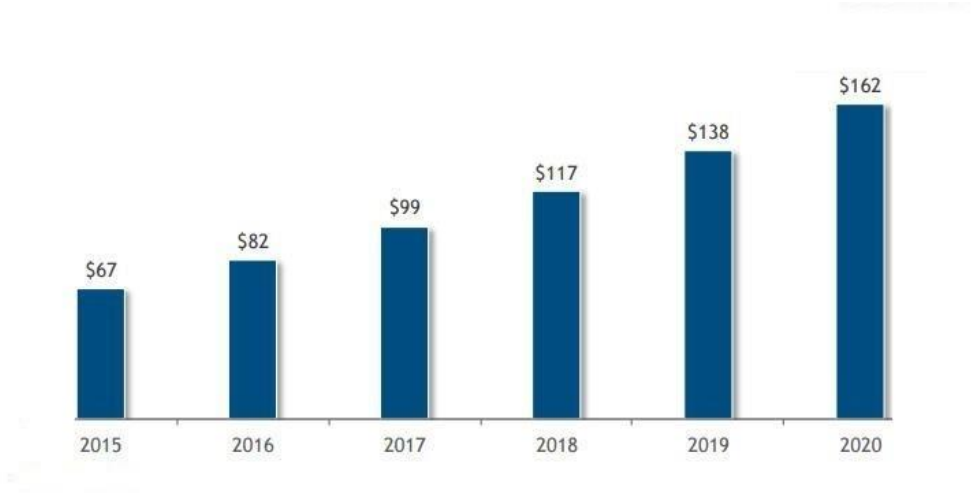

Fig. 5 *Worldwide Spending on Public Cloud Computing, 2015 – 2020 ($B)* *(3)*

All of the aforementioned led to the vast increase of data traffic and we entered the era of "**Big Data**", an era where anyone can analyze information and data in order to "extract more value" in human genomics, healthcare, oil and gas, search, surveillance, finance and many other areas. However, despite all the benefits, the surveillance of our personal data becomes a very easy task to anyone with the right tools and with the sheer amount of data, anyone will be able to make a detailed profile of our everyday lives.

2.3. The death of Privacy in the digital age

The "death of privacy" in the 21st century it is mainly inspired by accelerations in the development of technology [22] that lead to a vast increase of personal data storing and sharing. Additionally, it would appear from the widespread on-going debates that the human community, as a whole, still lacks the wisdom or ability to handle data fairly and justly, especially in terms of what should or should not be generated, stored shared and used. For example, social media users believe that convenience comes first and they will not hesitate to share personal identifiable information (PII) for the benefit of friends, which is obviously a false move when they are not in a position to know the intentions of many others that will be able to obtain their PII. One reason is the fact that social networks are still emerging [23]. Until they reach a mature state, privacy concerns will continue to pose problems. For example, consumers still trust their friends

more than any other source when it comes to researching a product, service or a topic. When looking at the rapid growth of social networks, it is worth noting that the three most popular social networks were launched less than 15 years ago. Their millions of users point to the public's desire to keep connected to their friends and coworkers. Therefore, some of the privacy issues can be attributed to the growing pains of the rapidly changing technological landscape.

As a result, such data is often subject to intentional or accidental information security breaches and can subsequently be accessed and interpreted by anyone capable of doing so, while at times also rendered available to others, including the general public. The effects of such breaches may also be exacerbated by rapid advances in data processing technologies, including in those enabling automatic and big data processing. As an additional example, information privacy breaches may contribute to physical privacy breaches, which refers to the unwanted access to human bodies and living spaces, such as when burglars are equipped with hacked personal data revealing the absence of occupants of a premise and/or the layout of the space and its infrastructure. In the digital age, individuals become increasingly vulnerable to privacy invasions as they depend more on the use of the Internet to carry out their daily activities and thus they disclose more of their personal data to others. The risk comes from both the fact that personal data becomes progressively digitized and as a result of it being stored in several devices and locations.

Mounting online threats include hacking, identity theft, fraud, phishing, pharming, spoofing, profiling, spyware, tracking cookies, online witch hunting, bullying and stalking, which may involve a wide range of actions, including the unwanted disclosure of a user's personal information (sometimes known as "doxing"). This can be achieved either through the subject's intentional or unintentional online activities and/or through others' uploading of the subject's digital information acquired offline—such as video images or sound tracks—in the absence of the subject's consent and/or outside the data subject's immediate control. Such privacy-invading actions can cause data subjects a wide variety of damages, including the prompting of suicidal thoughts or actions due to the victim's loss of critical elements of human life, such as safety, personal identity, autonomy and dignity. These examples are evidence of how traditional boundaries between the public and the private, between the physical and the virtual, and between the past and the present are collapsing.

3. DPIA

3.1. The History of DPIA

This section takes a chronological approach regarding to the concept of DPIA. Impact assessments and similar evaluation techniques have grown out of the emergence of new – and, at the time, not fully known – dangers to individual and collective societal concerns. They aim to address uncertainty and risk. For example, technology assessments (TAs) emerged in 1960s in the United States, initially as a tool used by scientists in order to better deal with the potentially dangerous consequences of their discoveries and inventions. They were subsequently institutionalized as a means to ensure – initially – product safety and have progressively encompassed a broader spectrum of issues relating to the society and technology. Likewise, environmental impact assessments (EIAs) surfaced as a response to the gradual degradation of the natural environment. Positive experience with both TAs and EIAs has aided their spread as practice worldwide and has resulted in proliferation, and sometimes institutionalization, of impact assessments in areas ranging from health care, regulation (governance), national security, surveillance practices to privacy and personal data protection.

The proliferation of privacy- (PIAs) and data protection- impact assessments (DPIAs) is attributed to three main factors:

I. the growing invasiveness of emerging technologies into individual lives and social fabrics
II. the increasing importance of the processing of personal data for contemporary economy, national security, scientific research and technological development, and inter-personal relations, among others
III. the diminishing trust in emerging technologies and the use thereof by public and private organizations.

However, some 50 years after impact assessments emerged, they still do not constitute a clear-cut practice. Only in certain areas have they gained considerable experience and matured (e.g. EIA). In other areas, their identities are still being developed (e.g. 'societal' impact assessments or DPIAs) and in other areas, calls for their introduction are constantly being made (e.g. human rights).

PIAs – and subsequently DPIAs – emerged in the 1990s and became institutionalized, in different forms and at various levels of compulsion, first in common law jurisdictions, such as New Zealand, Australia and Canada. In Europe, the earliest policy for PIA was developed in the United Kingdom in 2007. The EU has thus far put in place two sector-specific, voluntary PIA policies: the first for radiofrequency identification (RFID) applications (2009) and the second for 'smart grids' (2012). In the Better Regulation Package (2015), privacy and personal data constitute one of the many objects of assessment in the processes of EU law- and policy-making. After the adoption of both the GDPR and the Police and Criminal Justice Data Protection Directive (2016), a mandatory policy for impact assessment will be first introduced in the EU in May 2018 in the area of personal data protection[2].

3.2. Need of PIA

One of the instruments for safeguarding privacy is privacy impact assessment (PIA). There is growing interest in PIA and, consequently, it seems timely to publish what we believe is the first book on the subject. In Europe, the interest in PIA has been sparked by two main events. First was development and publication of a PIA handbook in the UK, the first in Europe, in December 2007. Second was the European Commission's Recommendation on RFID in May 2009 in which the Commission called upon the Member States to provide inputs to the Article 29 Data Protection Working Party for development of a privacy impact assessment framework for the deployment of radio frequency identification (RFID) tags. Article 4 of the European Commission's Recommendation on RFID said, "Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments. This framework should be submitted for endorsement to the Article 29 Data Protection Working Party within 12 months from the publication of this Recommendation in the Official Journal of the European Union." The RFID PIA Framework, developed by industry, was endorsed by the Art. 29 Working Party in February 2011. Since these two milestones, there have been frequent calls for PIA in Europe. The European Parliament, in its 5 May 2010 resolution on passenger name records (PNR), said that "any new legislative instrument must be preceded by a Privacy Impact Assessment and a proportionality test". European Commission Vice-President Viviane Reding said in July 2010 that "Businesses and

public authorities... will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a 'Privacy by Design' approach."

In its Communication of 4 November 2010, the European Commission said it will examine the possibility of including in its proposed new legal framework on data protection "an obligation for data controllers to carry out a data protection impact assessment in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance"[5].

Privacy by Design, as mentioned above, was developed by Former Ontario Information and Privacy Commissioner, Ann Cavoukian as an approach to privacy where privacy becomes an organization's default mode of operation and privacy is integrated into every step of their development processes. This means that privacy is embedded into product design and development to make sure the proper choices are available for people using the products, and the default options are the most privacy preserving.

Although Privacy by Design (PbD) was created independently from the GDPR, the GDPR adopts PbD in Article 25 which states that: "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

GDPR also requires an organization to keep records of their compliance activities to be able to demonstrate compliance (Article 24) and accountability (Article 5).

The PIA/DPIA is a critical operational tool, and record keeping tool to be able to demonstrate compliance with Articles 5, 24 and 25. The PIA must be operationalized and embedded into the product lifecycle so that it is triggered during the design process

of a product, and the PIA must include the proper set of questions to help the product designers analyze the proper privacy by design principles[5].

3.3. PIA & DPIA

3.3.1. Definitions

A Privacy Impact Assessment (PIA) is a questionnaire to identify and help reduce privacy risk. PIAs are fundamental to evaluating an organization's privacy activities, and to mitigating risks as efficiently as possible. PIAs are not only useful, but are oftentimes mandatory for privacy compliance. Privacy impact assessments can differ greatly in terms of scope, form, ways of being conducted, and even language. Companies across the world assess privacy impacts and potential risks of a process or product at the outset to comply with legal obligations or to ensure the quality of the product or services.

A Data Protection Impact Assessment (DPIA) is a specific type of PIA that is described in the EU GDPR and comes with unique obligations. With the new European General Data Protection Regulation (GDPR) coming into effect on May 25, 2018 companies must go through great changes regarding their privacy program, particularly how they handle their processing of personal data as well as their ability to demonstrate compliance.

Data protection impact assessments (DPIA) are addressed in the GDRP in Article 35, which states: "*Where a type of processing in particular using new technologies, and considering the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*"

In addition to Article 35 in GDPR, there are additional articles and recitals in the GDPR that are important to consider when implementing your DPIA process.

3.3.2. Why conducting a DPIA?

A DPIA has to be carried out on any complex or innovative processing of personal data or product whose stakes are high. In addition, according to GDPR it is also a legal obligation for an organisation to carry out a DPIA. Personal data are beyond

doubt valuable for the organisation that processes them, but this processing also creates a significant liability due to the risks concerning the rights and freedoms of data subjects. Furthermore, personal data have a value for others. This includes a market value if they are exploited for commercial purposes (spam, targeted advertising, etc.), or a nuisance value in the case of unfair actions (discrimination, denial of access to benefits, etc.) or malicious actions (fraudulent bank transaction, identity theft, blackmail threatening to destroy data, burglary, defamation, threats, assault, etc.).

Moreover, we can see phenomena that tend to change our view of threats: a culture of exposing our private life without worrying about the impacts this could have on our professional and social future, as well as increased capabilities of risk sources (structured criminal organizations and powerful tools easily found on the Internet, espionage between states, etc.). Personal data are therefore all the more vulnerable. Given the stakes that are often high, and the evolution of systems and threats, risk management enables to determine the necessary and sufficient controls. DPIA makes it possible to methodically study the processing of personal data or products, prioritize risks and treat them in a proportionate manner in order to mitigate the risks related to the rights and freedoms of the data subjects[13].

3.3.3. What are the benefits of conducting a DPIA?

Conducting a DPIA will improve awareness organisations of the data protection risks associated with a project. This will help to improve the design of the project and enhance the communication about data privacy risks with relevant stakeholders. Some of the benefits of conducting a DPIA are as follows:

- Ensuring and demonstrating that organisations complies with the GDPR and avoids sanctions.
- Inspiring confidence in the public by improving communications about data protection issues.
- Ensuring users are not at risk of their data protection rights being violated.
- Enabling organisations to incorporate **“data protection by design”** into new projects.
- Reducing operation costs by optimising information flows within a project and eliminating unnecessary data collection and processing.

- Reducing data protection related risks to organisations.
- Reducing the cost and disruption of data protection safeguards by integrating them into project design at an early stage[10].

4. Key Factors of DPIA

Within the context of the description of the DPIA key factors, a stock taking research revealed that the most widely accepted guidelines on DPIA are the Working Party 29 ones. The Article 29 Working Party (Art. 29 WP) is an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The composition and purpose of Art. 29 WP was set out in Article 29 of the Data Protection Directive, and it was launched in 1996. Its main stated missions are to:

- Provide expert advice to the States regarding data protection
- Promote the consistent application of the Data Protection Directive in all EU state members, as well as Norway, Liechtenstein and Iceland
- Give to the Commission an opinion on community laws (first pillar) affecting the right to protection of personal data
- Make recommendations to the public on matters relating to the protection of persons with regard to the processing of personal data and privacy in the European Community[7]

In April 2017, the Article 29 Working Party released guidelines on Data Protection Impact Assessment (DPIA). The guidelines were open for public comments until 23 May 2017 and the revised version was published in October 2017. The aforementioned guidelines were released in order to help organisations acquire a better comprehension on specific issues concerning the Data Protection Impact Assessment in practice. That need was created because the GDPR does not describe the whole process of conducting a DPIA in details. So this chapter identifies the answers to all the basic questions an organisation may have, regarding the conduct of a DPIA.

When is a DPIA mandatory?

The GDPR does not require a DPIA to be carried out for every processing operation which may result in risks for the rights and freedoms of natural persons. The carrying out of a DPIA is only mandatory where a processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1), illustrated by

Article 35(3) and complemented by Article 35(4)). It is particularly relevant when a new data processing technology is being introduced.

In cases where it is not clear whether a DPIA is required, the WP29 recommends that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers comply with data protection law.

Even though a DPIA could be required in other circumstances, Article 35(3) provides some examples when a processing is "*likely to result in high risks*":

- "*(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*

- *(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or*

- *(c) a systematic monitoring of a publicly accessible area on a large scale*".

As the words "*in particular*" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. There may be "high risk" processing operations that are not captured by this list, but yet pose similarly high risks. Those processing operations should also be subject to DPIAs. For this reason, the criteria developed below sometimes go beyond a simple explanation of what should be understood by the three examples given in Article 35(3) GDPR.

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to "*likely to result in a high risk*" processings, the following criteria should be considered:

1. Evaluation or scoring, including profiling and predicting, especially from *"aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements"* (recitals 71 and 91). Examples of this could include a bank that screens its customers against a credit reference database, or a

biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioral or marketing profiles based on usage or navigation on its website.

2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing "*legal effects concerning the natural person*" or which "*similarly significantly affects the natural person*" (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion

3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through "*a systematic monitoring of a publicly accessible area*" (Article 35(3)(c)). This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).

4. Sensitive data or data of a highly personal nature: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard, whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers

equipped with note-taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:

    a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
    b. the volume of data and/or the range of different data items being processed;
    c. the duration, or permanence, of the data processing activity;
    d. the geographical extent of the processing activity.

6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.

7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

8. Innovative use or applying technological or organizational solutions, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "Internet of Things" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.

9. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91). This includes processing operations performed in a public area that people passing by cannot avoid, or processing operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA. The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:

Examples of processing	Possible Relevant criteria	DPIA required?
A hospital processing its patients' genetic and health data (hospital information system).	- Sensitive data - Data concerning vulnerable data subjects	Yes
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring - Innovative use or applying technological or organizational solutions	Yes
A company monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.	- Systematic monitoring - Data concerning vulnerable data subjects	Yes
The gathering of public social media profiles data to be used by private companies generating profiles for contact directories.	- Evaluation or scoring - Data processed on a large scale	Yes
An institution creating a national level credit rating or fraud database.	- Evaluation or scoring. - Automated decision making with legal or similar significant effect. - Prevents data subject from exercising a right or using a service or a contract. - Sensitive data or data of a highly personal nature:	Yes
An online magazine using a mailing list to send a generic daily digest to its subscribers.	- Data processed on a large scale.	No
An e-commerce website displaying adverts for vintage car parts involving limited profiling based on items viewed or purchased on its own website.	- Evaluation or scoring.	No

Tab. 3 DPIA requirements

Conversely, a processing operation may correspond to the above mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, and include/record the views of the data protection officer.

In addition, a data controller subject to the obligation to carry out the DPIA "*shall maintain a record of processing activities under its responsibility*" including inter alia the purposes of processing, a description of the categories of data and recipients of the data and "*where possible, a general description of the technical and organizational security measures referred to in Article 32(1)*" (Article 30(1)) and must assess whether a high risk is likely, even if they ultimately decide not to carry out a DPIA.

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4)). The criteria set out above can help supervisory authorities to constitute such a list, potentially with more specific content added in time if appropriate. For example, the processing of any type of biometric data or that of children could also be considered as relevant for the development of a list pursuant to article 35(4).

Note: supervisory authorities are required to establish, make public and communicate a list of the processing operations that require a DPIA to the European Data Protection Board (EDPB) (Article 35(4)). The criteria set out above can help supervisory authorities to constitute such a list, with more specific content added in time if appropriate. For example, the processing of any type of biometric data or that of children could also be considered as relevant for the development of a list pursuant to article 35(4).

When isn't a DPIA required?

A DPIA is not required in the following cases:

a) where the processing is not "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1));
b) when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out. In such cases, results of DPIA for similar processing can be used (Article 35(1));
c) when the processing operations have been checked by a supervisory authority before May 2018 in specific conditions that have not changed;

d) where a processing operation, pursuant to point (c) or (e) of article 6(1), has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis (Article 35(10)), except if a Member state has stated it to be necessary to carry out a DPIA prior processing activities;

e) where the processing is included on the optional list (established by the supervisory authority) of processing operations for which no DPIA is required (Article 35(5)). Such a list may contain processing activities that comply with the conditions specified by this authority, in particular through guidelines, specific decisions or authorizations, compliance rules, etc. (e.g. in France, authorizations, exemptions, simplified rules, compliance packs…). In such cases, and subject to re-assessment by the competent supervisory authority, a DPIA is not required, but only if the processing falls strictly within the scope of the relevant procedure mentioned in the list and continues to comply fully with all the relevant requirements of the GDPR.

When shall the supervisory authority be consulted?

As explained above:

- a DPIA is required when a processing operation "*is likely to result in a high risk to the rights and freedoms of natural person*" (Article 35(1)). As an example, the processing of health data on a large scale is considered as likely to result in a high risk, and requires a DPIA;
- then, it is the responsibility of the data controller to assess the risks to the rights and freedoms of data subjects and to identify the measures envisaged to reduce those risks to an acceptable level and to demonstrate compliance with the GDPR (Article 35(7), see III.C.c). An example could be the storage of personal data on laptop computers with appropriate technical and organizational security measures (effective full disk encryption, robust key management, appropriate access control, secured backups, etc.) in addition to existing policies (notice, consent, right of access, right to object, etc.).

In the laptop example above, the risks have been managed by the data controller and following the reading of Article 36(1) and recitals 84 and 94, the processing can proceed without consultation with the supervisory authority. It is in cases where the data controller believes that reasonably available technologies and their implementation costs do not mitigate the risk (i.e. the residual risks remains high) caused by the processing operations, the applicable SA must be consulted, before such processing begins. An example of an unacceptable high residual risk includes where the data subjects may encounter significant, or even irreversible, consequences, which they may not overcome, and/or when it seems obvious that the risk will occur.

Whenever the data controller cannot find sufficient measures to reduce the risks to an acceptable level (i.e. the residual risks are still high), consultation with the supervisory authority is required.

Moreover, the controller will have to consult the supervisory authority whenever Member State law requires controllers to consult with, and/or obtain prior authorization from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health (Article 36(5)).

It should however be stated that regardless of whether or not consultation with the supervisory is required based on the level of residual risk then the obligations of retaining a record of the DPIA and updating the DPIA in due course remain.

What shall a data controller provide when consulting the SA?

The data controller should provide the Supervisor Authority with the following information

a) where applicable, the respective responsibilities of the controller**,** joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
b) the purposes and means of the intended processing;
c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the GDPR;
d) where applicable, the contact details of the data protection officer;

e) the data protection impact assessment; and
f) any other information requested by the SA.

Processors must assist data controllers, ensuring compliance with any obligations arising from a DPIA and from consultation with the SA[4].

What does a DPIA address?

A DPIA may concern a single data processing operation. However, Article 35(1) states that "*a single assessment may address a set of similar processing operations that present similar high risks*". Recital 92 adds that "*there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity*".

A single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks. Indeed, DPIAs aim at systematically studying new situations that could lead to high risks on the rights and freedoms of natural persons, and there is no need to carry out a DPIA in cases (i.e. processing operations performed in a specific context and for a specific purpose) that have already been studied. This might be the case where similar technology is used to collect the same sort of data for the same purposes. For example, a group of municipal authorities that are each setting up a similar CCTV system could carry out a single DPIA covering the processing by these separate controllers, or a railway operator (single controller) could cover video surveillance in all its train stations with one DPIA. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA has to be provided.

When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights of

the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations. Of course, the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific implementation, but this can be informed by a DPIA prepared by the product provider, if appropriate. An example could be the relationship between manufacturers of smart meters and utility companies. Each product provider or processor should share useful information without neither compromising secrets nor leading to security risks by disclosing vulnerabilities

Who is obliged to carry out the DPIA?

The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task.

The controller must also seek the advice of the Data Protection Officer (DPO), where designated (Article 35(2)) and this advice, and the decisions taken, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c)). Further guidance is provided in the next question 3.7 "What is the role of the DPO with respect to data protection impact assessments and records of processing activities".

If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.

The controller must "*seek the views of data subjects or their representatives*" (Article 35(9)), "*where appropriate*". The WP29 considers that:

- those views could be sought through a variety of means, depending on the context (e.g. a generic study related to the purpose and means of the processing operation, a question to the staff representatives, or usual surveys sent to the data controller's future customers) ensuring that the controller has a lawful basis for processing any personal data involved in seeking such views. Although it

should be noted that consent to processing is obviously not a way for seeking the views of the data subjects;

- if the data controller's final decision differs from the views of the data subjects, its reasons for going ahead or not should be documented;
- the controller should also document its justification for not seeking the views of data subjects, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies' business plans, or would be disproportionate or impracticable

Finally, it is good practice to define and document other specific roles and responsibilities, depending on internal policy, processes and rules, e.g.:

- where specific business units may propose to carry out a DPIA, those units should then provide input to the DPIA and should be involved in the validation process;
- where appropriate, it is recommended to seek the advice from independent experts of different professions (lawyers, technicians, security experts, sociologists, ethics, etc);
- the roles and responsibilities of the processors must be contractually defined; and the DPIA must be carried out with the processor's help, taking into account the nature of the processing and the information available to the processor (Article 28(3)(f));
- the Chief Information Security Officer (CISO), if appointed, as well as the DPO, could suggest that the controller carries out a DPIA on a specific processing operation, and should help the stakeholders on the methodology, help to evaluate the quality of the risk assessment and whether the residual risk is acceptable, and to develop knowledge specific to the data controller context;
- the Chief Information Security Officer (CISO), if appointed, and/or the IT department, should provide assistance to the controller, and could propose to carry out a DPIA on a specific processing operation, depending on security or operational needs.

What is the role of the DPO with respect to data protection impact assessments and records of processing activities?

As far as the data protection impact assessment is concerned, the controller or the processor should seek the advice of the DPO, on the following issues, amongst others:

- whether or not to carry out a DPIA
- what methodology to follow when carrying out a DPIA
- whether to carry out the DPIA in-house or to outsource it
- what safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of the data subjects
- whether or not the data protection impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with data protection requirements

As far as the records of processing activities are concerned, it is the controller or the processor, not the DPO, who is required to maintain records of processing operations. However, nothing prevents the controller or the processor from assigning the DPO with the task of maintaining the records of processing operations under the responsibility of the controller or the processor. Such records should be considered as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller or the processor.[7]

What about already existing processing operations? DPIAs are needed for those created after May 2018 or that change significantly

The requirement to carry out a DPIA applies to existing processing operations likely to result in a high risk to the rights and freedoms of natural persons and for which there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing.

A DPIA is not needed for processing operations that have been checked by a supervisory authority or the data protection official, in accordance with Article 20 of Directive 95/46/EC, and that are performed in a way that has not changed since the prior checking. Indeed, "Commission decisions adopted and authorisations by

supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed" (recital 171).

Conversely, this means that any data processing whose conditions of implementation (scope, purpose, personal data collected, identity of the data controllers or recipients, data retention period, technical and organisational measures, etc.) have changed since the prior checking performed by the supervisory authority or the data protection official and which are likely to result in a high risk should be subject to a DPIA.

Moreover, a DPIA could be required after a change of the risks resulting from the processing operations, for example because a new technology has come into use or because personal data is being used for a different purpose. Data processing operations can evolve quickly and new vulnerabilities can arise. Therefore, it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection in a changing environment over time. A DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, or new categories of data subjects become vulnerable to discrimination. Each of these examples could be an element that leads to a change of the risk resulting from processing activity concerned.

Conversely, certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated or if a monitoring activity is no longer systematic. In that case, the review of the risk analysis made can show that the performance of a DPIA is no longer required.

As a matter of good practice, a DPIA should be continuously reviewed and regularly re-assessed. Therefore, even if a DPIA is not required on 25 May 2018, it will be necessary, at the appropriate time, for the controller to conduct such a DPIA as part of its general accountability obligations.

Should the DPIA be published?

Publishing a DPIA is not a legal requirement of the GDPR. It is left upon the controller´s decision. However, data controllers should consider publishing their DPIA, or perhaps part of their DPIA. The purpose of such a process would be to help foster trust in the controller’s processing operations, and demonstrate accountability and

transparency. It is particularly good practice to publish a DPIA where members of the public are affected by the processing operation. This could particularly be the case where a public authority carries out a DPIA.

The published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller or give away trade secrets or commercially sensitive information. It could even consist of just a summary of the DPIA's main findings.

Moreover, when a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority (Article 36(1)). As part of this, the DPIA must be provided (Article 36(3)(e)).

At what moment should a DPIA be carried out? Prior to the processing.

The DPIA should be carried out "prior to the processing" (Articles 35(1) and 35(10), recitals 90 and 93). This is consistent with data protection by design and by default principles (Article 25 and recital 78). The DPIA should be seen as a tool for helping decision-making concerning the processing.

The DPIA should be started as early as practical in the design of the processing operation even if some of the processing operations are still unknown. As the DPIA is updated throughout the lifecycle project, it will ensure that data protection and privacy are considered and promote the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses because the selection of certain technical or organizational measures may affect the severity or likelihood of the risks posed by the processing.

The fact that the DPIA may need to be updated once the processing has actually started is not a valid reason for postponing or not carrying out a DPIA. In some cases the DPIA will be an on-going process, for example where a processing operation is dynamic and subject to ongoing change. Carrying out a DPIA is a continual process, not a one-time exercise.

5. DPIA Methodology

Records of Processing Activities

Prior conducting a Data Protection Impact Assessment, it is necessary for the organisation to create a Record of Processing Activities. Article 30 of the GDPR obliges organisations to maintain "*records of processing activities*". The shorter term "processing records" is also used which is based on the earlier term "processing directory". The legal status (until 25.05.2018) already required a register of proceedings (*processing directory*), which, in part, should be available for examination to anyone upon request. Often, in practice, different terms were used for this legally required documentation. Formerly, the term "public processing directory" was used for the documentation intended for public information; in practice and in literature, the terms "public registry" and "processing directory" were coined. The GDPR does neither provide to the public the right to access the registry nor command the obligation for the company's procedures to be registered. Therefore, the distinction between "public" and "internal" is no longer necessary. However, the supervisory authority can request the processing records. As the processing records can be extended in order for some meaningful documentation to be added - without being legally required - the term "extended processing records" will be used.

The processing records serve to ensure transparency with regard to processing personal data and to provide legal protection for the company. It can support the company's data protection officer, as well as the supervisory authority in carrying out their tasks. In accordance with Article 30 paragraph 4 of the GDPR, the controller or the processor shall make the record available to the supervisory authority upon request. The processing records also serve as verification, so the company can prove to the supervisory authority that the requirements of the GDPR were fulfilled by the controller. Part of the general duty of the controller is the cooperation with the supervisory authority upon request in the performance of its tasks (Article 31 of the GDPR). The processing records are therefore not only the basis for fulfilling the controller's or processor's managerial duties, but also support the data protection officers in fulfilling their tasks.

Obligation to Maintain Processing Records

The obligation to maintain processing records is stipulated in Article 30 of the GDPR. According to Recital 82 the record is used as proof for compliance and demonstration of accountability with the GDPR rules. The scope of the obligation to documentation covers all processing activities of the controller. In principle, every controller is subject to the obligation to maintain such a record of processing activities. While two or more controllers, who have joint control over the purposes and means of processing, are so called "joint controllers", not every one of them is obligated to maintain the records himself. Rather, joint controllers can conclude an agreement on which of them has to fulfill which obligations of the GDPR, and can therefore also determine who maintains the records. The processor also has to maintain records on all categories of processing activities carried out by the processor on behalf of the controller[14].

The GDPR presents a broad, generic framework for designing and carrying out a DPIA and sets out the minimum features of a DPIA (Article 35(7), and recitals 84 and 90):

- "a description of the envisaged processing operations and the purposes of the processing"
- "an assessment of the necessity and proportionality of the processing"
- "as assessment of the risks to the rights and freedoms of data subjects"
- "the measures envisaged to:
- "address the risks";
- "demonstrate compliance with this Regulation".

As mentioned above, the GDPR does not prescribe the exact process for carrying out a DPIA, allowing for flexibility and scalability in line with your organisation's needs. Although there is no one prescribed approach to take, the following steps are considered as a guideline of conducting a DPIA:

5.1. Identifying whether a DPIA is required or not;

In this first step, the data controller needs to decide whether a DPIA must be conducted or not. As it is mentioned in chapter 4 above, the GDPR require a DPIA to be carried

out for every processing operation is "*likely to result in a high risk to the rights and freedoms of natural persons*" (Article 35(1)). However, in cases where it is not clear whether a DPIA is required, the data controller should take into consideration the 9 criteria of the WP29 before take the final decision. The data controller will also need to identify the resources needed, the individuals who will be involved, and the timeframe of the DPIA process.

5.2. Describing the information flows

At an early point in the DPIA procedure, it should be identified how it is intended to collect, store, use and delete personal information as part of the project. This exercise should also identify what kinds of information will be used during the DPIA procedure and who will have access to the information.

The aim of this step is to get an early understanding of how information will be used at each step along the procedure. This is crucial to being able to recognise the data privacy risks which are posed by a processing operation and to identifying what actions will mitigate those risks.

It should be considered if any new personal information will be generated by the project, and include it in the record of this stage. For example, a project involving the processing of psychometric tests might take one type of personal information (the answers to psychometric test questions) and process it to another (a psychometric profile). This new type of personal data is different in character, and so recording it separately in the map of information flows, will help to ensure that its special characteristics are taken account of, later in the DPIA process.

At this stage of the DPIA procedure, internal stakeholders as well as external partners may be consulted with a view to identifying the technical and organisational aspects of information collection, storage and processing. The aforementioned external partners may be engaged by the organisation as a data processor. This exercise should be documented using whatever means are most suitable for the organisation and the processing operation concerned. Using visual aids, such as flow charts, to document how information will be used, might assist in identifying potential data privacy risks. This may also help with internal communication by better allowing the project team and others in the organisation to understand the design of the processing operation.

5.3. Identifying data protection and related risks

This stage involves examining the design of the processing operation in order to assess what data protection issues arise, and to identify any risks it may expose individuals to, as well as any data privacy-related risks that the process might create for the organisation.

There are a range of different ways that an individual's data privacy can be compromised or put at risk by a new process. The types of risk range from the risk of causing distress, upset or inconvenience, to risks of financial loss or physical harm. There are equally as many kinds of data privacy-oriented risks to organisations, as compliance-oriented issues and commercial factors. Breaches of the GDPR, such as excessive data processing or data breaches, can lead to significant penalties, as well as causing reputational damage to organisations.

This step should build upon work done at previous stages of the DPIA. The responses to the criteria laid out in the above section "How do I know if a DPIA should be conducted" should act as a guide to the risks which may be present. The map of information flows generated in stage 5.2 may help you to identify particular weak spots, where general data privacy risks are likely to be particularly acute, or which might give rise to specific risks. Examples of the risks related to individuals should be considered at this stage of the DPIA process and are outlined below. Sector-specific guidance, which may be provided by regulators or industry groups in your area of operations, should be also examined.

Furthermore, the magnitude of the risks identified should be taken into consideration, having regard to both their likelihood and impact. In assessing the severity of the risk, it is important to bear in mind:

- the sensitivity of the personal data,
- the number of people likely to be affected by any of the risks identified
- and how they might be affected.

A record of all risks identified at this stage will assist later on the DPIA process, by creating solutions to avoid or reduce those risks. Record keeping may be especially important in the event of an investigation or audit by the DPA. Good record keeping may help to demonstrate how the organisation complied with its obligations under the GDPR.

This identification exercise should be carried out relatively early in the process design, as mentioned in the previous chapter, having in mind the sooner that data privacy risks can be identified, the easier and cheaper it will be to mitigate them. However, it is not a once-and-for-all exercise and the process design should be kept under review throughout the DPIA process to monitor the emergence of any new risks, which may occur by a change to the design or scope of the processing operation.

The organisation can choose the risk management approach that best suits its existing project management process. The key point is to ensure that a methodological approach to identifying risks is adopted, and records of this process are accurately kept.

Example Risks To Individuals

- Inappropriate disclosure of personal data internally within your organisation due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment by organisation's personnel may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by "hackers".
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the process.
- Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.

- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the process may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Conclusively, along with the risks related to individuals, the organisation may face risks of prosecution, significant financial penalties, or reputational damage if fails to comply with the provisions of the GDPR. Failure to carry out a DPIA, where appropriate, is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new processing operation may bring.

5.4. Identifying and evaluating data protection solutions

This stage follows on, from the identification of data protection risks at stage 5.3, with the aim of minimising the data privacy risk associated with the process. In almost all cases, it will be possible to eliminate data privacy risks completely. However, under GDPR, if there are remaining high risks, then you will need to consult with the Data Protection Authority, as described below. Data Protection solutions, which are able to act as mitigating actions, are steps that may be taken to reduce the likelihood or severity of data privacy risks being identified.

During this stage, data protection solutions should be identified to reduce the impact of the risks. This should be conducted by reducing each risk individually or by implementing a privacy solution my address a number of risks together.

The nature of these privacy solutions will depend on the types of risk that have been identified. Moreover, it should be assessed whether a particular privacy solution should be pursued, in terms of cost and benefits.

At this stage, it should be also ensured that the process will be in compliance with data protection laws. In particular, it should be considered whether the processing operation complies with the data protection principles, and ensuring that all the personal data processes are based on a firm legal basis.

5.5. Signing off and recording the DPIA outcomes

The primary aim of conducting a DPIA is to identify and minimize or eliminate the data privacy risks involved in a process. The GDPR requirement, about the high risk areas of the Record of Processing Activities, is to conduct a Data Protection Impact Assessment on them. This means that the organisation should have registered the risks, their mitigating actions and the methodology that was implemented for extracting these outcomes.

If the privacy risks which have been identified are not capable of mitigation and it would not be proportionate to accept them, this stage should be used for re-evaluating the viability of the process. In such circumstances, an organisation may decide to either change the process, or abandon it.

5.6. Integrating the DPIA outcomes back into the project plan

Once it has been signed off, the organization should put the outcomes of the DPIA into action by integrating any necessary changes into the plans of the compliance project.

As part of the implementation of the DPIA, it should be assessed whether the privacy solutions implemented, intend to mitigate the relevant privacy risks. Additionally, if the processing operation change or expand over its lifetime, it may be necessary to assess whether a further DPIA is required or not. Such a review can be built into the organisation's existing procedures[10].

6. DPIA Difficulties & Troubleshooting

It is a fact that the process of conducting a DPIA might be very difficult and there can be many complications and obstacles during their performance, due to the fact that there are no clear, strict and standardized rules and guidelines for their implementation. Moreover, the lack of staff and stakeholders privacy awareness can further implicate things.

One of the most important factor that is mainly responsible for the integrity and consistency of the DPIAs is determining the proper way to weigh different risk/impact estimates and balancing risk/impact categories. The vast variety of different business processes throughout an organization may lead business owners to calculate the risk/impact level not in a standardized way. This happens because in some cases there are no determined criterias for assessing the risk/impact level and thus it can result to subjectively and ill-defining the risk/impact level.

There are many ways to identify these risk/impact level criteria and a proper definition of them might be the following:

Impact rating	Descriptor	Operational			Reputational		Financial
		Customers	Business Systems and Operations	Employees	Stakeholders	Brand	Revenue and Cost
5	Intolerable	More than 50% of customers have been negatively affected.	Business is unable to operate due to significant loss of systems.	More than 50% of the workforce is affected.	Formal regulatory intervention and fines.	Negative national and international media coverage.	Revenue loss of in excess of 10% of revenue.
		Large scale customer loss.	Disruption to the business requiring significant additional unbudgeted resource and the attention of the Crisis Management Team.	Significant negative impact on employee experience.	Impacts stakeholders with strategic relevance (Government, Shareholders, and Strategic Partners).		Financial loss is unacceptable to management and /or can only be recovered in the long term (over 3 years).
			Significant impact on internal parties.		Direct Senior Management/Board involvement.		
4	Major	25-50% of customers have been negatively affected.	Business continues to operate with a major loss of systems.	Impacts between 25%-50% of our workforce.	Formal regulatory investigation or enquiry.	Negative national and limited international media coverage.	Revenue loss of in excess of 5% but less than 10% of revenue.
		Serious customer loss.	Disruption to the business requiring additional unbudgeted resources and the attention of Senior Management.	Negative impact on employee experience.	Senior Management involvement		Financial loss is major and/or can only be recovered in the medium term (3 years).
			Major impact on internal parties.		Major impact on working relationships with key stakeholders, including external parties.		
3	Significant	Large scale customer complaints.	Business continues to operate with a moderate loss of systems.	Impacts on up to 25% of the workforce.	Informal regulatory enquiry.	Limited negative national media coverage.	Revenue loss of at least 2.5% but less than 5% of revenue.
		A degree of customer loss.	Disruption to the business requiring unbudgeted resources.		Senior Management involvement.		Financial loss is moderate and/or can only be recovered within 1 year.
			Significant impact on internal parties.		Moderate impact on working relationships with key stakeholders, including external parties.		
2	Moderate	Increase in customer complaints.	Business continues to operate. Minor loss of systems with no additional resources required.	Minor impact on employee experience.	Impact on working relationships with a minor working or third party relationship.	Limited negative local or industry media coverage.	Revenue loss of in excess of 1% but less than 2.5% of revenue.
1	Minor	Slight increase in customer complaints.	Business continues to operate. Insignificant loss of systems.	There is no or an insignificant impact on employee experience.	Insignificant impact to stakeholders.	No negative media coverage.	Revenue loss of less than 1% of revenue.

Tab. 4 Risk/impact level criteria

Some criteria might be more suitable for the processes of an organization but they might not apply for a different kind of organization. The most important thing

though, is that an organisation should select the same criteria for assessing the risk/impact level of all its business processes[46].

Furthermore, an organisation might make the mistake of conducting the DPIAs after the completion of the business process, at the end of the process design or even later, when the process is already up and running. The appropriate moment for conducting a DPIA is during the creation of the process, because conducting the DPIA at a later stage may result to high cost, complex and time consuming changes at the business process.

Another mistake occurs where solely the legal department is responsible for conducting the DPIA. The most appropriate approach would be the involvement of the legal department along with the IT, Privacy and Information Security departments. While conducting the DPIA, not all the answers that should be provided will typically be known by the legal department, so it will need to involve the key stakeholders from IT, Information Security and Privacy. It is also important to mention, that these answers, provided by the aforementioned departments, must be as detailed as possible, in order to accurately calculate the risk level.

The most common misconception concerning the DPIA is the fact that in case a PIA has been conducted there is no need for a DPIA. This occurs because there is a belief that there is no clear and notable distinction between the two. However, this is wrong because the term DPIA is explicitly defined in the GDPR, and includes specific record keeping obligations that are unique. Many organizations who have existing PIA processes in place think that they are compliant and incorrectly be under the impression that they already meet the DPIA obligations of GDPR. The term DPIA should be reserved and strictly used only when the DPIA triggers in the GDPR are met, and specific care must be taken to record the DPIA in a GDPR compliant format.
Furthermore, it must be noted that conducting a DPIA is not a one-time process. DPIAs should be performed during the change of a process and also during the establishment of a new process. It is also highly advisable to perform DPIAs periodically, the period of which is recorded in the policy of each organisation[12].

Critics have argued that impact assessments constitute an unnecessary burden, adding to already overgrown bureaucracy, causing unnecessary expenditure and delays in decision-making, or even slowing the entire development process. Thus, it is no surprise that there is a recurrent wish for impact assessments to be quick, simple and cheap. Moreover, critics underline the complexity of the assessment process in practice,

the difficulties it brings, along with a lack of practical experience and minimal or non-existent guidance and oversight. They further question their added value over other evaluation techniques, e.g. compliance checks, as well as their efficacy, pointing out the broad discretion often afforded as to whether and how such impact assessments should be conducted. Impact assessments are often criticised for their seemingly 'lip service' nature, being used solely to comply with a regulatory requirement, for their conduct only with the least amount of effort, or for their instrumental use, being used only to legitimise intrusive initiatives.

Additionally, organisations sometimes focus on conducting assessments only for the regulatory protection they provide without using them as a mean to address the impact of their envisaged initiatives. They often confuse impact assessments with audits. Organisations inaccurately consider the consequences solely pertaining to themselves (e.g. reputational, business or financial risks), rather than assessing also the consequences for individuals and the public at large. Ultimately, impact assessments are often performed too late, i.e. when the design of an initiative cannot be meaningfully influenced anymore[2].

7. Conclusion

It is undeniable that there is a clear level of subjectivity when conducting a DPIA. However, there are guidelines that try to make things clear and try to provide a level of certainty for DPIA's outcomes. Despite the fact that the performance of the DPIAs can be confusing and time consuming, they provide a clear assurance to data subjects that their rights and freedoms are protected. Conclusively, an organisation by conducting a DPIA under the right conditions and at the appropriate time, will have two-sided benefit. That is because the organisation along with the compliance that will be able to demonstrate, will be also able to provide assurance to data subjects that their rights and freedoms are properly protected. This means that the organization will comply with GDPR's obligation to conduct DPIAs and will take into consideration any possible risk affecting data subjects.

8. References

[1] R. Clarke. (2009, April). "Privacy impact assessment: its origin and development." *Computer Law & Security Review.* [Online] 25 (2), pp. 123-135.

[2] Vrije Universiteit Brussel (2017) "Data protection impact assessments in the European Union: complementing the new legal framework towards a more robust protection of individuals"
Available online at: https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf

[3] Paul de Hert, Vagelis Papakonstantinou," The new General Data Protection Regulation: Still a sound system for the protection of individuals?", 2016

[4] Taylor Wessing, Exploring data protection impact assessments, 2016
Available online at: https://united-kingdom.taylorwessing.com/globaldatahub/article-exploring-data-protection-impact-assessments.html

[5] David Wright, Paul de Hert, Privacy Impact Assessment, Springer

[6] Roger Clarke, 'The Distinction between a PIA and
a Data Protection Impact Assessment (DPIA) under the EU GDPR', For a Panel at CPDP, Brussels, 27 January 2017
Available: http://www.rogerclarke.com/DV/PIAvsDPIA.html

[7] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether
processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (October. 4, 2017)

[8] Official site of OneTrust | Privacy Management Software Available: Available: https://onetrust.com/article-29-working-party-issues-revised-guidelines-data-protection-impact-assessment-dpia/

[9] ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Data Protection Officers ('DPOs') (October. 4, 2017)

[10] Data Protection Commisioner Site
Available: http://gdprandyou.ie/data-protection-impact-assessments-dpia/

[11] Λίλιαν Μήτρου, «Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, ωέο δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα», Δίκαιο & κοινωνία στον 21ο αιώνα, 2018

[12] Rebecca Herold," GDPR: What a Data Protection Impact Assessment Is and Isn't"
Available online at: https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=864

[13]CNIL," PRIVACY IMPACT ASSESSMENT (PIA)",2015

[14]Bitkom," The Processing Records",2017
Available online at: http://www.mittelstand-tour.de/bitkom/org/noindex/Publikationen/2018/Leitfaeden/180530-Verzeichnis-von-Verarbeitungstaetigkeiten-nach-Art-30-EU-Datenschutz-Grundverordnung-DS-GVO/180529-LF-Verarbeitungsverzeichnis-ENG-online-final.pdf

[15] European Parliamentary Technology Assessment. (2009, March) *"What is a Technology Assessment."* [Online]. http://www.eptanetwork.org/EPTA/what.php, [Nov. 30, 2009]

[16] M. Barrett. (2003, June). "Environmental impact statement." *Omega.* [Online]. 7 (5), pp. 431-
439. Available: http://www.sciencedirect.com/science/article/B6VC4-48TTM96-5J/2/773df09b6a1d2455faeca8d67d622776, [Nov. 28, 2009].

[17] Justia. "Robertson v. Methow Valley Citizens, 490 U.S. 332 (1989)." Internet: http://supreme.justia.com/us/490/332/case.html, June. 06, 2009 [Nov. 30, 2009].

[18] International Association for Impact Assessment. . "Principles of Environmental Impact
Assessment Best Practice." Internet:
http://www.iaia.org/publicdocuments/specialpublications/Principles%20of%20IA_web.pdf,
Jan. 1999 [Dec. 1, 2009]

[19] G. Beanlands. *"Environmental Impact Assessment: Theory and Practice",* 5th ed, P.Wathern
Ed, Great Britain, Routledge, 2004, pp 31-85

[20] T. Dixon. (1997, January). "Communication Law Centre wants IPPs revised in line with
Australian Privacy Charter." *Privacy Law & Policy Reporter.* [Online]. 3(9), reference 5.
Available: http://www.austlii.edu.au/au/journals/PLPR/1997/4.html, [Dec. 16, 2009].

[21] B. Stewart. (1996, June). "PIAs – an early warning system." *Privacy Law & Policy Reporter*.
[Online]. 3 (7), pp. 45-49 Available:
http://www.austlii.edu.au/au/journals/PLPR/1996/65.html,
[Oct. 26, 2009].

[22] Simson Garfinkel, (2001) Database Nation: The Death of Privacy in the 21st Century, Sebastopol: O'Reilly Media.

[23] S. Srinivasan , ISACA journal volume 6 2012, Lack of Privacy Awareness in Social Networks, available online at:
https://www.isaca.org/Journal/archives/2012/Volume-6/Documents/12v6-Lack-of-Privacy-Awareness.pdf

[24] Details of Treaty No.005, Convention for the Protection of Human Rights and Fundamental Freedoms, Available online at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=7&DF=11/12/2014&CL=ENG

[25] Universal Declaration of Human Rights, Available online at: http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

[26] Solove D. J., "The digital person: Technology and Privacy in the information age", NYU Press, 2004. Available online at: http://dx.doi.org/10.1016/j.clsr.2017.05.021

[27] Robin Doherty , Jan 6 2016, rdoh, Why privacy is important, and having "nothing to hide" is irrelevant, Available online at: https://robindoherty.com/2016/01/06/nothing-to-hide.html

[28] Anna Romanou, Athens' Law Bar Drève de Nivelles 145, bte 36, 1150 Brussels, Belgium, "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", Available online at: www.sciencedirect.com

[29] Daniel Solove, Teach Privacy, January 10 2014, "10 Reasons Why Privacy Matters", Privacy and Security Blog, Available Online at: https://www.teachprivacy.com/10-reasons-privacy-matters/

[30] Richard L. Villars, Carl W. Olofson, Matthew Eastwood, June 2011, IDC Analyze the Future, "Big Data: What it is and why you should care"

[31] James S. Huggins' Refrigerator Door, "How Much Data Is That?", Available Online at: http://www.jamesshuggins.com/h/tek1/how-big.htm

[32] Paula Doe, SEMI, SemiconWest Beyond Smart, "Consumer to Industrial Data Explosion Hits Supply Chain", Available online at: http://www.semiconwest.org/consumer-industrial-data-explosion-hits-supply-chain

[33] "A Comprehensive List of Big Data Statistics," Wikibon Blog, 1 August 2012, Available online at: http://wikibon.org/blog/big-data-statistics/

[34] "eBay Study: How to Build Trust and Improve the Shopping Experience," KnowIT Information Systems, 8 May 2012, Available Online at: https://research.wpcarey.asu.edu/?utm_source=knowwpcarey&utm_medium=referral%2Farticle.cfm%3Faid%3D1171

[35] Jacob Morgan, Forbes 13 May 2014, "A Simple Explanation of IoT", Available online at: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1410d5a61d09

[36] Buyaa, R., Yeo, C. S., (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), 599-616

[37] Official Journal of the European Union, 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), Available online at: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[38] ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ, Hellenic Data Protection Authority, http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL

[39] Fieldfisher, "Privacy, Security and Information Law, http://privacylawblog.fieldfisher.com/2015/getting-to-know-the-gdpr-part-1-you-may-be-processing-more-personal-information-than-you-think/

[40] European Union Agency for Network and Information Security, ENISA web site, Data Protection – Privacy by Design, Available online at: https://www.enisa.europa.eu/topics/data-protection/privacy-by-design?tab=details

[41] "Data mapping under the GDPR and beyond", 2016 Baker & McKenzie LLP, Available Online at: http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Data%20Mapping%20under%20the%20GDPR%20and%20Beyond.pdf

[42]ICO, Data Protection Impact Assessment
Available online at: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf

[43]Κωνσταντίνος Λιμνιώτης (Αρχή Προστασίας Προσωπικών Δεδομένων), «Η σημασία της εκτίμησης επιπτώσεων στην προστασία των προσωπικών δεδομένων», 28/1/2015

[44] Baker & McKenzie LLP,"Data Protection Impact Assessment Under the GDPR",2016

[45] Felix Bieker,"A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation",Springer,2016

[46] Rolf H. Weber*," Privacy management practices in the proposed EU regulation", Oxford University Press, 2014