UKRAINIAN CATHOLIC UNIVERSITY

Faculty of Social Sciences

Department of Theory of Law and Human Rights

GDPR Documentation

Masters in Human Rights

Student

Illia Pidhainyi

Supervisor:

Markiyan Bem

Reviewer:

Ivan Horodyskyi

Lviv, Ukraine

2019

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Art(s).	Article(s)
CJEU (or the Court)	the Court of Justice of the European Union
CNIL	the Commission nationale de l'informatique et des libertés
DPA	Data Protection Authority
ECHR	the Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR (or the Court)	the European Court of Human Rights
EDPB	the European Data Protection Board
EU	the European Union
EEA	the European Economic Area
GDPR, the Regulation	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)
ICO	the Information Commisioner's Office
WP29	the Article 29 Working Party

INTRODUCTION

The General Data Protection Regulation – data protection law of the European Union and the European Economic Area, which was adopted on 14 April 2016, and came into force on 25 May 2018. The Regulation aims to protect personal data of individual citizens of the EU and the EEA, ensures the free movement of data throughout the EU, and establishes rules for the movement of personal data outside the EEA.

The two years were intended to allow to prepare to the application of the General Data Protection Regulation. However, uncertainty in approaches to compliance issues still exists.

Companies shall "undertake appropriate measures to comply with provisions of the Regulation." The GDPR itself does not list such measures or describe criteria of appropriateness. Therefore, it gives margin of appreciation for companies in their choice of such measures. One of the measures may be documentation.

In 2018, with the entry into force of the GDPR, the Internet community formed several misinterpretations. Dozens of websites assured that only two documents – data protection policy and privacy policy - would be enough to comply with the GDPR. Such a statement distorted understanding of entrepreneurs or even lawyers of compliance measures as well as of relevance and variety of documentation.

The definition of documentation is broader than just documents and also includes ongoing processes or other actions to be conducted or recorded in time – as an instruction. Documentation may be a part of a recording of data and related information or may establish procedures necessary to comply with the GDPR.

Aim of this paper – to identify specific documents as an appropriate measure for compliance with the Regulation and how to adopt them in business processes. This research may be used to help business executives or lawyers in the management of short-term (e.g., collection of personal data) and long-term (e.g., organization of storage of personal data) needs of their company.

The main **objectives** of this master thesis are the following:

— to identify the position of documentation in compliance with principles of processing personal data;

— to analyze relevant data protection law and requirements or approaches to creation and use of documents;

— to identify the necessary content of policies, records, and other documents and to suggest recommendations on how to adopt them in the business process.

The **object** of this research is the process of complying with the provisions of Regulation by adopting documentation. The **subject** of this research is the list of documents to be adopted to comply with the provisions of Regulation.

The methodology of this thesis *i.a.* involves:

1. the method of observation – research and study of the relevant legislation, case law, commentaries, and opinions;
2. the method of analysis (in particular of the legislation, its interpretation by the EU bodies and authorities of the EU Member States, opinions and publications on data protection, documentary analysis);
3. legal impact analysis – record and explanation of how the GDPR works within its scope;
4. induction – used to reach conclusions and formulate recommendations given the legal provisions, their relevance, and application.

Key **sources** of this thesis are:

The General Data Protection Regulation and Recitals to it, the law of the European Union, case law of European Court for Human Right (ECHR) and of the Court of Justice of the European Union (CJEU), opinions and publications of data protection authorities, academic publications other articles about data protection.

Structure

The thesis is composed of the introduction, three chapters, conclusions and the list of sources.

CHAPTER I
DOCUMENTATION AS A PART OF COMPLIANCE

1.1 Importance of GDPR

Data is the new oil © Clive Humby, mathematician

Top-5 most significant data breaches are the following:

1. Yahoo, 3 bln, and 500 mln affected people. 2013 and 2014, respectively. Reason – hacking.

2. First American Financial Corp., 885 mln affected people, 2019. Reason – poor security.

3. Facebook, 540 mln affected people, 2019. Reason – poor security.

4. Marriott International, 500 mln affected people, 2018. Reason – hacking.

5. Friend Finder Networks, 412.2 mln affected people, 2016. Reason – poor security/hacking.[1]

Poor security caused three of the five most significant data breaches.

It is almost impossible to count how many millions of people were affected by misuse or mistreating their personal data all over the world. Such misuse includes, for example, handing or even selling data to third parties (Facebook and Cambridge Analytica case, as the most recent famous case).

What is the value of personal data?

Personal data – is information, which helps to identify a natural person. For big companies, it is especially valuable because of profiling.

Profiling is a processing of personal data for evaluating a person`s past, present, and future - “performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements."[2] This information helps companies improve their advertising and marketing, offering goods or services to person individually. Predicting purchases of your consumer – the most straightforward way for the prosperity of business.

---

[1] CNBC, 5 of the biggest data breaches ever: https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html

[2] General Data Protection Regulation, Art. 4(4)

In some situations, personal data are: poorly secured, badly structured, badly access-restricted by big companies – controllers or processors of this data.

Unfortunately, one of the reasons for the current situation - the cheapness of data. Almost all consumers and users consented to give companies their personal data free of charge, and companies` expenses in this scenario – costs on processing and storing personal data (it means that companies are not paying to data subjects for their data).

This factor influences both natural persons and companies. Individuals – because of cheapness (personal data deemed as not valuable property), and post-processing control by a person overusing and storing his or her personal data - almost does not exist. A person simply does not care who, how, and why uses his/her personal data.

Thus, if the data subject does not care about personal data, business cares even less — possession of almost free assets with a sustainable increase in value – seems to be a profitable business. Indeed, personal data sets could be deemed as highly liquid assets – if society looks on personal data as an asset.

However, even without trading purposes, unfortunately, it is widespread practice – inappropriate handling of personal data without security measures required by new technologies or without a simple understanding of how to treat personal data of the company's employees.

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 – most known as General Data Protection Regulation – contains a means for the solution of problems mentioned above.

The Regulation entered into force on 25 May 2018, causing turbulence amongst business and their lawyers with compliance officers/departments. The main reason for that, in the author`s opinion, is the absence of prescribed or established a way to comply with it. Furthermore, the GDPR compliance is a set of continuous processes, which require incorporating the Regulation provisions in ongoing business activities.

Why the GDPR is important?

1. The Regulation protects people and their privacy.

As mentioned above, personal data are helping businesses with increasing levels of sales by offering more suitable goods or services.

Often, the use of personal data is hidden under a veil (even corporate), and data subject are just not interested in that, because of impossibility to find out the truth.

However, the GDPR gives every person instruments for control over personal life. They were called "data subject rights."

Chapter 3 establishes the following rights of a data subject:

– right of access by the data subject[3] (to send a request to the company, and demand information about the use personal data by a company or third parties);

– right to rectification (a data subject may ask the company for addition or alteration of personal data about him/her if it is uncompleted or something else) [4];

– right to erasure (another name - to be forgotten) (right of a data subject to immediate demand deletion of his or her personal data. One of the basis – when personal data have been unlawfully processed) [5];

– right to data portability (right of the subject to send a request to transfer personal data from controller to another controller – and the company should be ready to send information without delays);

– right to object – meaning objection of a data subject to processing his/her personal data. In this case, the company may no longer process data unless it demonstrates legitimate grounds for the processing. [6]

Is has a powerful impact on companies, activities of which may be publicized. Such provisions existed before the Regulation; however, a combination of the rights with establishment of enforcing system makes companies obey on some occasions. Thus, apart from legislative protection, the GDPR provides self-defence means, which ensures privacy.

---

[3] GDPR, Art. 15
[4] Ibid, Art. 16
[5] Ibid, Art. 17
[6] Ibid, Art. 21

2. Legislative technique of the GDPR concentrates on nature rather than form.

The Regulation was written in vague language.

It means that it does not contain provisions with a list of actions to be done or a list of documents to be prepared. Companies are free in their actions to comply with the GDPR.

To be precise, "free in their actions" means that the burden of assessment of personal data case lies upon controller or processor. This assessment will be a basis for choosing a compliance path: which documents to prepare, how to store and protect data.

A company shall assess a situation and make a decision – for example, about the legal basis to be used, amount and types of personal data to be collected, organisational and security measures to be taken. For all of these examples corresponding provisions on lawfulness of processing, storage and purpose limitation, security principle, respectively apply.

This assessment and decision-making approach differs from a typical compliance approach, if not in nature - in scope. Provisions as "*the controller shall take **appropriate** measures"* are often used in the Regulation.

Why this approach is the next step? It is because of avoiding long lists of situations and solutions to them. A company has only guiding principles to be followed and assessment approach. Naturally, it caused more problems, more expenses on compliance, not all companies are conducting it properly. Still, it is an effective mechanism for data protection.

3. The GDPR – data protection law, required in the 21-st century.

"The digital universe is doubling its size every two years. In 2020 it reaches 44 zettabytes – 44 trillion gigabytes."[7]

A legal act sometimes becomes obsolete after a year or two of coming into force. One of the reasons – rapid developing of technologies. It is beyond power of legislative authorities to predict technological progress.

[7] EMC, Executive Summary Data Growth, Business Opportunities, and the IT Imperatives: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

The Regulation has not been amended since adoption – 14 April 2016, despite data protection requires security measures like clouds, SaaS, access-restrictions means, and other rapidly developing technologies.

This problem was solved “by imposing on companies an obligation to implement *appropriate* technical and organisational measures to ensure a level of security *appropriate* to the risk.” [8]

There is an assessment approach, mentioned above, and it solved the technology problem – companies by themselves decide, what technology to use considering their obligations and risks to the confidentiality of personal data (and expenses, of course).

In Art. 32.2 some technology-based measures were mentioned - pseudonymisation and encryption. [9]

4. The Regulation is working.

Law shall establish not only a legislative framework but also enforcement and responsibility system.

In the GDPR, this system includes Data Protection Authorities (DPA), compliance system and fines.

DPA – is a national authority responsible for the implementation of the Regulation in a Member State and authorised to impose fines (or issuing warnings).

Under the GDPR two types of fines may be imposed:

- “up to 10 million EUR, or up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher";[10]

- “up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher".[11]

Evaluating existing cases, the GDPR is doing his job – slowly, but effectively. Nowadays, DPA of the Europe starting proceedings against companies, including GAFAM members (Google fined for 50 mln Euro by French data protection

---

8 GDPR, Art. 32(1)
9 Ibid, Art. 32(3)
10 Ibid, Art. 83(4)
11 Ibid, Art. 83(5)

authority).[12]

Data protection compliance, considering its importance, can not be simple. As a law, it requires drafting and adopting documentation. However, the GDPR has its own approach to documentation issues, and important role plays corporate (for internal use) documents.

What is "GDPR documentation"?

In definition "GDPR documentation," was put the meaning of:

1) documentation, directly or indirectly listed in articles or recitals of Regulation;

2) documentation that deemed necessary or advisable to use to comply.

The Regulation contains no statements like "you shall write these two policies, and this obligation will be fulfilled." On the contrary, it has compliance provision, and it is controller`s decision how to comply with it – whether by writing 1 or 100 documents or skip this option at all.

It is uneasy to list all documents, which were created after 25 May of 2018 by lawyers or supposed-to-be-a-lawyer persons. As of now, websites offer dozens of policies "to be GDPR-complied," despite their true content and compliance role being unexplained to the user. These websites used hype on GDPR, emerged in spring 2018, and offer unreliable legal services.

It was one of the many reasons why I decided to write a master thesis about data protection documentation.

All documentation to be mentioned in this dilpoma may be classified in the following categories:

1. Keystones

The most important documents will be listed here. They are either frequently used by companies in relation to the data subject or are essential for infiltrating data protection compliance rules in the internal processes of a company. The most important documents are:

[12] THEVERGE, Google fined €50 million for GDPR violation in France: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

- privacy notice (frequently nicknamed on the Internet as "privacy policy") – literally, this is a notification from a company to user, that his or her personal data will be collected, on what basis, and recipients of personal data. The privacy notice shall be delivered to the data subject "at the time when personal data obtained." [13] It is allowed to put privacy notice on your website. Privacy notice in electronic form is standard practice.

- data subject consent form – according to Art. 6.1, consent is a lawful basis for processing personal data. Consent shall be expressed by data subject in clear affirmative act, with unambiguous agreement on consent terms. Consent shall be in oral, written, or electronic form. By the way, the company may submit to the user consent form, so the user does not have to draft document and only sign it. This way leads us to the company's obligation to draft this consent with precise information and in plain language.

The frequency of using consent as a lawful basis for the processing of personal data increases the value of consent as a legal act and, also, as a document.

- data protection policy – apart from the importance of this document for internal processes of a company, this document has often been published on the website of the company as a manifesto to users or consumers for ensuring them about the confidentiality and safety of their personal data.

Data protection policy in its public part should contain contact details of the company, principles, and purposes of the processing, third parties as recipients of personal data. Also, it would be useful to describe rights of the data subject and ways of using these rights (how a company should treat request about access to information or erasure of data)

Data protection policy in its internal part will be a central document, determining principles of data processing and implementing them in routine processing activities.

- records management policy – this policy is a real keystone, yet it is not so popular as data protection policy.

---

[13] GDPR, Art. 13

This policy shall describe processes around personal data as information to be collected, maintained, updated, and stored.

Policy is going to be a central document for staff, handling personal data. This document would be extensive. For example, its typical provisions would cover:

– gathering data and putting it into the register of personal data;

– reasons for the review of the registers;

– established ways of deleting or anonymizing personal data, with links to the retention schedule.

2. Records and registers

Most known records are the following:

- **a record of processing activities** – this is documented information about every action with personal data, done by a company. Specifically, the type of personal data, from who, how, and why it was collected. Also, it contains contact details of the controller or joint controller or processor, as well as contacts of data protection officer.

The obligation of keeping records of processing activities stated in Art. 30. The records shall be in writing and electronic form. Considering the obligation of mentioning every single processing operation and a direct stating of obligation, it draws a lot of a company's attention and, especially, resources.

Furthermore, the controller has an obligation for demonstration of compliance [14], and records of processing activities, apart from compliance, are essential for demonstration of compliance too. Demonstration of compliance clause may involve such provisions, as, for example, the lawfulness of processing, purpose limitation, and data minimisation.

In this case, the supervisory authority in requested records shall see a lawful basis and purpose for collecting personal data. Records of processing activities provide necessary information – how much of personal data company gathered, whether a company needs such data at all, did the user consent for this, did the company received too much information or not.

[14] GDPR, Art 5(2)

- **records of consent**. As established in Art. 7.1 of the Regulation, "where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data." [15]

Consent may be in oral, written, or electronic form. For a demonstration of compliance, for every existing form of compliance shall be records, in particular, audio records - for an oral form, archive - for written form, and store information on a cloud or elsewhere - for electronic form. In brief, register of consent shall contain the following information: who and when consented, what they were told at that moment (text of consent), how they consented, and whether they have withdrawn consent.

- **a register of data breaches** – according to Art. 33, personal data breach shall be reported to the supervisory authority immediately (not later than 72 hours);[16] and without undue delay – to the data subject. Art. 33 also stated an explicit obligation of the controller – "to any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."[17]

It is a crucial document and it shall be treated with the biggest carefulness possible because of the sensitivity of related actions. Data protection authority (DPA) may not impose a fine on a company because of hacking, however, because of poor security – it must. Documenting the effects of data breaches requires proper assessing of people affected by a personal data breach. As mentioned above, data breaches could affect dozens or hundreds of millions of data subjects.

Therefore, register of data breaches, which may be requested by the supervisory authority and properly checked, and information for the register shall be subject to expert analysis.

3. Policies

- **data breach policy** – is an instruction for employees in case of data breach. It is common practice that the first action shall be a minimization of harm to already leaked personal data. Next step – evaluating the danger of data breach in the whole

[15] GDPR, Art 7(1)
[16] Ibid, Art. 33(1)
[17] Ibid, Art. 33

personal data system (for example, if unlawful access to personal data was possible because of security vulnerability – the direction is to find and fix this vulnerability in the whole system).

After this, the controller shall send notifications to the supervisory authority and data subjects affected by a data breach. Also, the company shall file information about the data breach to the data breaches register.

Apart from these actions, data breach policy shall contain other measures in their public or private part (public – for example, press-releases) concerning data breaches.

- Data subject request policy – is a policy describing the process of responding by the company to request of the data subject. Such requests are provided by Chapter 3 of the Regulation about data subject rights.

According to Articles 15, 16, 17, 21 of the GDPR, a person has right of access to information, concerning him; right to amend and delete information about him in possessing of company.

Controller shall know the way of responding to such requests and obeying them (how to ensure complete alteration of personal data, or comprehensive deletion, etc.)

Importance of this policy highlighted by the fact that infringements of data subject`s rights, according to Article 83.5(b) of the Regulation entails more severe fines, that other provisions. [18]

- Data transfer policy – Regulation's scope covers the territory of the European Union and protecting residents of EU (even from non-EU companies). Also, it foresees the possibility of transferring personal data outside the EU (not the same, as processing of personal data by non-EU company).

Transferred personal data still protected by the Regulation requiring even more security measures from both controller and third-party.

Therefore, this policy shall contain provisions about steps of the company by transferring personal data, depending on whether it based on an adequacy decision, with safeguards or as an exemption. An important part of transfer is an explanation of

[18] GDPR, Art. 83(5)(b)

choosing a path for transferring personal data and purposes of such transferring (is transfer really necessary for company).

- **Employee data protection policy.** Almost all of companies have a need for this policy. Employees are a special category because their personal data are being collected on an ongoing basis, and it involves many more issues than in processing in relationship "controller – data subject". For example, "in case law of the European Court of Justice recordings of work times which include information about the time when an employee begins and ends his workday, as well as breaks or times which do not fall in work time, [considers] as personal data."[19] Furthermore, the annual assessment of performance or surveys can be personal data too.

Also, companies, as employers, shall carefully choose the legal basis of processing. Consent of employee shall be freely given – meaning an employer shall pull no pressure on new employee.

Employer should set in policy rules for collecting of personal data from employee, including notification about collecting, purposes of collecting, authorized access to personal data, etc.

4. Other

- Data retention schedule – is a document, which prescribed the future of personal data in possessing of company.

It means that controller shall determine the period (in years or months), for how long it stores personal data, and what it shall do when this period expires. Retention period should be determined for every category of data, collected by company.

The Regulation contains no explicit provisions like "medical records shall be stored for 5 years". However, Art. 5.1.(e) of the GDPR stated that: "personal data shall be kept (...) for no longer than is necessary for the purposes for which the personal data are processed."[20] Controller shall resort to the assessment approach and set retention period with a margin of appreciation.

Retention schedule should contain: category of personal data; trigger action

[19] Article 29 Working Party, Personal Data: https://gdpr-info.eu/issues/personal-data/
[20] GDPR, Art. 5(1)(e)

(what caused beginning of retention period), final action (review, delete or anonymise), etc.

- Data breach notification is a text of a message from controller to the supervisory authority or to data subject, whose personal data has been compromised (leaked or hacked).

Considering the provision of Article 34.1, that notification shall be communicated to data subject without undue delay, a draft of notification should be prepared for immediate use.

The notification shall describe the following: "the nature of the personal data breach, communicate the name and contact details, describe the likely consequences of the personal data breach, and the measures taken or proposed to be taken by the controller." [21]

Summary

Documents may be similar in content, but different in approach. Some documents should be drafted for immediate sending (privacy notice or data breach notification). Some of them are to be published - so, they have to be written in explicitly clear language for users. Some of them should be maintained on a long-term basis.

Therefore, documents and provisions related to them shall be described, understood and assessed in the light of time expenses for preparing thereof – considering both content of a document and other elements, accompanying it.

1.2 Scope of the Regulation

Compliance with the Regulation begins from determining whether processing activities fall under the scope of the Regulation. It is possible that the EU company is not obliged by the GDPR, and that non-EU company shall comply.

Therefore, issues of the scope of the operation of the GDPR will be examined in the first place.

Scope of the operation of the GDPR has two parts – material and territorial.

Material scope

[21] GDPR, Art. 33(3)

The Regulation, as a legal act, is intended to protect personal data. Who is data subject, as defined in the Regulation, and what personal data are or are not protected, described in Article 2 – the Material scope of the Regulation.

Art. 2.1 prescribed the following:

"This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." [22]

Filing system, according to Art. 4.6 means:

"any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;"[23]

A filing system is closely connected to documentation, specifically – to a register (depository) of personal data.

Recital 15 pointed out for two important tips:

"In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used." [24]

It is an important clause considering the importance of data protection law in the 21-st century. Data are growing in price, big data are growing at a high price. Personal data of a million people, located near to each other, give local companies tremendous benefit in sales. Such an amount of data can be collected only by automatic means, which means that those should subject to limitations.

"Files or sets of files, as well as their cover pages, which are not structured according to specific criteria, should not fall within the scope of this Regulation." [25]

This clause, as vice versa of Art. 2.1, give us a valuable hint – small companies can avoid the Regulation if data processing activities are unsystematised, as well as records about them and personal data as data set are unstructured (these two things are

[22] GDPR, Art. 2(1)
[23] Ibid, Art. 4(6)
[24] Working Party 29, Recital 15 to the General Data Protection Regulation
[25] Ibid

often linked).

Art. 2.2 indicated that:

"Regulation does not apply to the processing of personal data:

a. in the course of an activity which falls outside the scope of Union law (activities regarding national or common security)" [26]

"b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

c. by a natural person in the course of a purely personal or household activity;

d. by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." [27]

Also, the Regulation does not apply to:

- legal persons (contact details) [28];

- criminal prosecutions (personal data, collected for purposes of prevention, investigation or prosecution of criminal offences)[29];

- personal data of deceased persons.[30]

Territorial scope

The territorial scope has two elements, and if only one is present, the Regulation shall apply in this matter.

Art. 3.1 of the Regulation reads as follows:

"This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not." [31]

Of course, there are almost no doubts about the scope of operation of the Regulation over the EU companies. However, there is a challenge – to determine whether or not data processing activities of non-EU companies regulated by the

[26] Working Party 29, Recital 16 to the General Data Protection Regulation
[27] GDPR, Art. 2(2)
[28] Working Party 29, Recital 15 to the General Data Protection Regulation
[29] Working Party 29, Recital 19 to the General Data Protection Regulation
[30] Working Party 29, Recital 27 to the General Data Protection Regulation
[31] GDPR, Art. 3(1)

European data protection law.

Moreover, it is a fundamental issue for legal advice with regard to GDPR-compliance matters.

Article 3.1 has an essential definition of an "establishment", which helps in answering questions of the application of the GDPR.

Recital 22 described a definition of "establishment" as follows:

"Establishment implies the effective and real exercise of activity through stable arrangements." [32]

The CJEU, in its decision, expanded the definition of an establishment:

"establishment - any real and effective activity — even a minimal one — exercised through stable arrangements." [33]

"Stable arrangements", especially in case of online services company, may constitute quite a low threshold for application of the Regulation to the company.

The European Data Protection Board, in its guideline on the territorial scope, expresses the opinion, according to which:

"the existence of an establishment within the meaning of the GDPR should not be interpreted too broadly to conclude that the existence of any presence in the EU with even the remotest links to the data processing activities of a non-EU entity will be sufficient to bring this processing within the scope of EU data protection law."[34]

For assessing whether the company has or does not have an establishment, the EDPB offers two criteria:

- "Relationship between a data controller or processor outside the Union and a local establishment in the Union;

- Revenue raising in the Union".[35]

Nature and scope of links between non-EU companies and the EU will be a keystone for determining whether the Regulation applies to the company's data processing activities or not.

---

[32] Working Party 29, Recital 22 to the General Data Protection Regulation

[33] Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság (C- 230/14) Judgement of the Court of Justice of the European Union

[34] Guidelines 3/2018 of European Data Protection Board on the territorial scope of the GDPR (Article 3), p.6

[35] Guidelines 3/2018 of European Data Protection Board on the territorial scope of the GDPR (Article 3), p.7

Territorial scope, in its second part, has another nature – meaning, it describes not a company, but its business activities, and, of course, its connection with data processing.

Targeting criteria of territorial scope are prescribed by Art. 3.2 the GDPR:

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

1. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or

2. the monitoring of their behaviour as far as their behaviour takes place within the Union." [36]

These clauses need a detailed analysis:

- "such data subjects in the Union" - "data subjects, on purposes of Regulation, are natural persons, whatever their nationality or place of residence, concerning the processing of their personal data". [37]

- "offering goods or services." Again, there is room for analyse of business processes of the company. Recital 23 stated that:

"In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union." [38]

The Regulation does not explain what offering goods or services shall be deemed as "apparent". Several non-cumulative criteria are indicating whether a company is targeting natural persons, defined as data subjects, or not. Examples may include offering delivery to the Member States or targeting in advertisement EU residents as consumers by plain text.

The EDPB's Guidelines provide examples of apparent offering:

- "The data controller or processor pays a search engine operator for an internet

---

[36] GDPR, Art. 3(2)
[37] Working Party 29, Recital 14 to the General Data Protection Regulation
[38] Working Party 29, Recital 23 to the General Data Protection Regulation

referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience

- The international nature of the activity at issue, such as certain tourist activities;

- The mention of dedicated addresses or phone numbers to be reached from an EU country;" [39]

- "The use of a language or a currency other than that generally used in the trader's country, especially a language or currency of one or more EU Member states;" [40]

Thus, two or three of these elements combined lead to a conclusion, that offering goods or services to the EU residents indeed takes place. However, some particular examples do not prove offering beyond reasonable doubt.

This point is affirmed by Recital 23.3, stating that mere accessibility of the company's website to the EU residents in not enough to entail the application of the Regulation based on the territorial scope. However, "language and currency of Union or Member State, possibility of ordering and providing of delivering – will be considered as an apparent offering of goods and services."[41]

If it is apparent that the company is offering goods or services, "controller and processor should designate a representative, which should act on behalf of the controller or the processor and may be addressed by any supervisory authority".[42]

- "monitoring of their behaviour" - another way of falling under the scope of Art. 3.2.

First of all, "their behaviour" means the behaviour of data subjects, as clarified in Recital 14.

Secondly, the behaviour of a natural person falls under a definition of profiling, stated in Art. 4(4) the GDPR.

---

[39] Guidelines 3/2018 of European Data Protection Board on the territorial scope of the GDPR (Article 3), p.15
[40] Ibid, p.16
[41] Working Party 29, Recital 23 to the General Data Protection Regulation
[42] Working Party 29, Recital 80 to the General Data Protection Regulation

Recital 24 described a way of identifying monitoring activities:

"In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to make decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours, and attitudes." [43]

Examples of monitoring behaviour are the following:

- cookies;
- geolocation tracking;
- behavioural advertising;
- CCTV.

Summary

Scope of the Regulation is a critical issue for business all over the world. Not every European company will fall under its scope, and not every non-EU company is excluded from it. Compliance has it preliminary part – when company assesses, whether or not its processing activities similar to activities, described in Art. 2 or 3 of Regulation.

As mentioned above, existing only one activity, which stated by provisions of Art. 3.1 or Art. 3.2, leads to falling of the company's data processing under the territorial scope, therefore the GDPR applies.

Such activities are:

- creating a filing system of personal data and structuring it by specific criteria;
- offering goods or services to a natural person, located in the EU – use the EU or Member State currency and language, offering delivery within the EU.
- use of cookies or other tracking tools against the EU residents – proper cookie policy, with provision about limitation of targeting.

To sum up, the main principle of jurisdiction scope is the protection of people in Europe. Collecting personal data for business purposes will be certainly

[43] Working Party 29, Recital 24 to the General Data Protection Regulation

encompassed by GDPR.

Scope of the Regulation is a flexible legal tool. The inherent vagueness of provisions in conjunction with the overwhelming importance of the issue lead to the necessity of precise describing of the material and territorial scope of the Regulation.

1.3 Nature of accountability principle

Accountability is not a box-ticking exercise © ICO.

Every legal act has its system of reporting, as well as a particular way of compliance with it. So does the GDPR.

Art. 5 stated: "the controller shall be responsible for, and be able to demonstrate compliance with, [principles relating to the processing of personal data]" [44] (accountability principle).

This provision clearly imposes compliance obligation on every person having to comply with Regulation under Art. 2 or 3.

For a better understanding of the accountability principle and what has documentation to do with compliance, the accountability will be viewed with academic and legal approaches.

Place of accountability principle in the Regulation

The keystone of the principle lies in Art.5.2, cited above.

Apart from this, the Regulation often casually mentions "compliance" or "demonstration of compliance" on some issues: corporate codes, certifications.

Important provision about compliance is stated in Art. 24:

"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." [45]

---

[44] GDPR, Art. 5
[45] GDPR, Art. 24(1)

"Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller." [46]

Paragraph 1 indicates what compliance is – implementing appropriate technical and organisational measures.

There are other provisions connected with the accountability principle:

- Recital 78 – "Appropriate technical and organisational measures"; [47]

- Art. 28 – "Processor."

It explains the burden of accountability in case of engaging processors:

"that controller shall use only providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation." [48]

- Art. 32 – "Security of processing"[49]

This Article provides examples of organisational and technical measures to ensure the security of processing.

- Art. 25 – "Data protection by design and by default" [50] – how to choose and implement measures to meet the requirements of the Regulation.

- Art. 83 – Conditions for imposing administrative fines.[51]

Overall, the accountability principle is enshrined in every clause, which mentions an obligation of the company to do something (even if an obligation exists in a provision such as "to implement appropriate measures".

Place of accountability principle in European data protection law and case-law

Law. For the first time accountability principle appeared in 1980 in the international law, established by the Organisation for Economic Co-operation and Development - "Recommendation of the Council concerning Guidelines governing the

[46] Ibid, Art. 24(2)
[47] Working Party 29, Recital 78 to the General Data Protection Regulation
[48] GDPR, Art. 28
[49] Ibid, Art. 32
[50] Ibid, Art. 25
[51] Ibid, Art. 83

protection of privacy and transborder flows of personal data". Principle was defined as follows:

"A data controller should be accountable for complying with measures which give effect to the principles stated above." [52]

Compared to the provision in the GDPR, it is not identical. However, they are similar in linking compliance – controller shall comply with data protection principles.

Before the GDPR, the primary document in European data protection law was Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

This Directive has no explicit provision with a definition of accountability principle. However, paragraph 25 stated, that "principles of data protection must be reflected in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing". [53]

In other words, the principles are the basis for obligations imposed on companies. This is a similar provision to accountability principle; however, this principle was not amongst data protection principles generally.

The General Data Protection Regulation substituted the Directive.

In 2009, European data protection authorities, in cooperation with the Centre for Information Policy Leadership started discussions on accountability in data protection law. These discussions were further called "Accountability project."

The project, started by Irish Data Protection Commissioner, was named as "Galway project". The Galway paper identified crucial elements of the accountability principle:

"1. Organisational commitment to accountability and adoption of internal policies consistent with external criteria.

2. Mechanisms to put privacy policies into effect, including tools, training, and

---

[52] Organisation for Economic Co-operation and Development (OECD), “Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data”, para. 14

[53] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, para. 25

education.

3. Systems for internal ongoing oversight and assurance reviews, and external verification.

4. Transparency and mechanisms for individual participation, and

5. Means for remediation and external enforcement." [54]

Simultaneously, the Spanish Data Protection Authority drafted its project of Madrid Resolutions. It was adopted in 2009 on the International Conference of Data Protection and Privacy Commissioners.

This Resolution, in section 11, provided the meaning of the accountability principle:

"Accountability principle. The responsible person shall:

a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and

b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers".[55]

Both Irish and Madrid projects divided the accountability principle in two parts – compliance and demonstration of compliance. Such an approach was also used in the GDPR yet in other words.

The Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010 by Article 29 Data Protection Working Party, explained the essence of the accountability principle in detail.

In the Opinion, WP29 said, that "particularly in the on-line environment, personal data has become the *de facto* currency in exchange for on-line content."[56]

The Opinion recognised increasing social, political and business value of personal data, and importance of data protection, especially – accountability.

Working Party 29 advanced a particular proposal for a general provision on

---

[54] Center for Information Policy Leadership, "Data Protection Accountability: The Essential Elements A Document for Discussion", 11-14

[55] International Conference of Data Protection and Privacy Commissioners, "International Standards on the Protection of Personal Data and Privacy – The Madrid Resolution", 5 November 2009

[56] Working Party 29, Opinion 3/2010 on the principle of accountability

accountability, which reads as follows:

“Article X - Implementation of data protection principles

1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.

2. The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request” [57]

Overall, the Opinion evaluated existing in 2010 data protection law and accountability provisions and concluded that Directive 95/46 requires improvement.

Recommendations contained in the Opinion were taken into account in the General Data Protection Regulation.

Case-law. Court decisions play an important role in forming, interpreting and applying data protection law.

Decisions of the European Court of Human Rights

The European Convention on Human Rights in Article 8 stated that: "Everyone has the right to respect for his private and family life, his home and his correspondence." [58]

Personal data was recognized by the Court as an integral part of the right to privacy of a person in Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland: "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention." [59]

According to p. 67 of the judgement in case S. and Marper v. the United Kingdom:

"In determining whether the personal information retained by the authorities involves any of the private-life aspects, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of

[57] Working Party 29, Opinion 3/2010 on the principle of accountability
[58] European Convention on Human Rights, Art.8(1)
[59] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, 27 June 2017, ECtHR

the records, the way in which these records are used and processed and the results that may be obtained." [60]

Court hearing cases about violation of privacy by States, specifically – public entities or other public actors. Despite such cases are not covered by the topic of this master thesis, the case-law of ECtHR is relevant to current data protection law and useful in processing personal data – in looking into current data processing practice and broadening or narrowing scope of the right on privacy.

Acting as an institution within the framework of the Council of Europe, the ECtHR influences European law, especially given that the Court applying living instrument in its case-law. For example, the practice of the ECtHR may set obligations for Members of the European Union and other parties to the ECHR concerning direct or indirect data protection actions.

Direct actions, *e.g.*, are lawful processing of personal data by public entities of the country (according to https://edpb.europa.eu/news/national-news_en, data protection authorities of Member States impose fines for infringement of the GDPR on public entities too). [61]

Indirect actions – the adoption of legislation and policies aimed at the protection of personal data.

In Z v. Finland the Court stated that: "The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article." [62] As stated in Gardel v. France, "The domestic law should ensure that such data are relevant and are efficiently protected from misuse and abuse."[63]

In its decision in case I v. Finland, the Court examined a failure of State to investigate, whether unlawful access to health register took place. Regarding the obligation to ensure security and integrity the Court said that:

---

[60] S. and Marper v. the United Kingdom [GC], § 67, Applications nos. 30562/04 and 30566/04, 4 December 2008, ECtHR

[61] EDPB, National News [about fines under GDPR]: https://edpb.europa.eu/news/national-news_en

[62] Z v. Finland, § 95, Application no. 22009/93, 25 February 1997, ECtHR

[63] I v. Finland, Application no. 20511/03, 17 July 2008, ECtHR

"Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life".[64]

Thus, Member States have obligations to protect personal data beyond those stated by the Regulation.

Another example of the ECtHR's practice influence is broadening of definitions of personal data or principles of processing.

What can be deemed as personal data, according to the Court:

1. GPS information ("real-time geolocation of the applicant's vehicle by means of a GPS device");[65]

2. "A DNA profile contains substantial amounts of unique personal data";[66]

3. "Banking documents undoubtedly amount to personal data concerning an individual, irrespective of whether or not they contain sensitive information"; [67]

4. Metadata (for example, time and duration of phone calls).[68]

To sum up, the Convention brings to personal data additional protection by establishing the right to privacy. In terms of data protection, the ECtHR's decisions serve as an additional legal instrument for better understanding of data protection law at all and broaden and explain obligations of Member States for keeping a person's privacy secure.

Even though only applications against states are considered admissible by the ECtHR, infringement of the GDPR may lead to a fine imposed by both data protection authority and the Court separately. For example, it may be the case if a public entity failed to investigate, prevent or report the data breach.

---

64 Ibid

65 Ben Faiza v. France, no. 31446/12, 8 February 2018, ECtHR

66 S. and Marper v. the United Kingdom [GC], § 75, Applications nos. 30562/04 and 30566/04, 4 December 2008, ECtHR

67 M.N. and Others v. San Marino, § 51, no. 28005/12, 26 April 2012, ECtHR

68 Malone v. United Kingdom, no. 8691/79, 2 August 1984, ECtHR

Therefore, case-law of ECtHR should be considered as a part of European data protection law.

The Court of Justice of the European Union

There are several decisions of the CJEU concerning data protection.

In case "College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboe" the Court examined possible unlawful access to medical records and failure of State to protect sensitive data.[69]

The Court in its decision stated the following:

"It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller." [70]

The Court, in its decision, broadened the definition of "access to information" and indicated the ways for the fulfilment of the obligation by a State.

In Patrick Breyer v. Bundesrepublik Deutschland, the Court ruled, that dynamic IP address, with additional data, can be deemed as personal data:

"However, it must be determined whether the possibility to combine a dynamic IP address with the additional data held by the internet service provider constitutes a means likely reasonably to be used to identify the data subject." [71]

In another case, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, the Court issued a decision about cookies consent:

"Article 4(11) and Article 6(1)(a) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 (General Data Protection Regulation), must be interpreted as meaning that the consent referred to in those provisions is not validly

---

69 College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, C-553/07, CJEU

70 Ibid

71 Patrick Breyer v. Bundesrepublik Deutschland, p. 37, C-582/14, CJEU

constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent."[72]

Prohibition of the use of pre-ticked boxes is stated not in Articles of Regulation, but in Recitals. In this decision, the Court emphasized such prohibition and explicitly stated its position on this issue.

In its decisions, the Court of Justice of the European Union:

- forms case-law in data protection law;
- draws attention to proper compliance with provisions of the Regulation;
- explain or stress obligations of controller or processor in specific personal data issue.

1.4 Rules of accountability

What accountability principle means?

Art. 5.2 of the Regulation contains two parts of the accountability principle:

1. compliance;
2. demonstration of compliance.[73]

Both are separate processes and require significant efforts.

1. Compliance is the approach of a company to put business activities in a legal framework.

The GDPR has its unique approach – data protection by design and by default, established by Art. 25 of the Regulation:

"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 organisational measures, such as pseudonymisation, which are designed to implement

[72] Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, C-673/17, CJEU

[73] GDPR, Art. 5(2)

data-protection principles, such as data minimisation, 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." [74]

Data protection by design and by default – cornerstone of the Regulation, and is going to be mentioned in this thesis more and more as a key to understanding what company should or should not do with personal data.

The Opinion of the ICO about data protection by design and by default enlightens these two provisions.

"Data protection by design is ultimately an approach that ensures you consider privacy and data protection issues at the design phase of any system, service, product or process, and then throughout the lifecycle."[75]

In other words, the controller should infiltrate respect to consumer's privacy in every action with personal data. It concerns not only lawyers or the very persons, who are in contact with consumers. It has a broad impact over staff, including C-level.

"Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose.

Data protection by default requires the controller to put in place the appropriate technical and organisational measures designed to implement the data protection principles."[76]

One of the data protection principles – accountability principle.

Technical measures are not considered (at least, in this chapter), so the focus is on organisational measures.

Organisational measures may be considered as appropriate if “they are taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.”[77]

Examples of this organisational measures, according to the ICO, are:

- “adopting and implementing data protection policies;

---

[74] GDPR, Art. 25(1)

[75] ICO, Data protection by design and default: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

[76] Ibid

[77] GDPR, Art. 24(1)

- taking a 'data protection by design and default' approach;

- putting written contracts in place with organisations that process personal data on your behalf;

- maintaining documentation of your processing activities;

- recording and, where necessary, reporting personal data breaches;

- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests".[78]

Respective authority indicates that documentation is one of the compliance actions. Even more, it defined three types of documentation described above: policies, records of data breaches, and records of processing activities as organisational measures for compliance with the Regulation.

Documentation and its role in compliance in general

Why documentation is an appropriate measure?

Documentation may be an appropriate measure to comply or demonstrate compliance with the specific provision and specific obligation. It heavily depends on the nature of the obligation, for example:

- to provide information instantly – privacy notice or data breach notification. Both documents are supposed to contain unique information. However, in case of a plurality of recipients it will be useful to create a template of document.

- to store information – register of data breaches or records of consent. Both documents serve as proof of compliance. Creating a central depository of these records will encourage to systematise information and ease demonstration of compliance by request.

- to do something – for example, records management policy describing the process of storing personal data in general.

The Opinion of WP29 on the principle of accountability describes the role of the accountability as the controller's obligation to:

- "put in place measures which would – under normal circumstances –

[78] ICO, Accountability and governance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

guarantee that data protection rules are adhered to in the context of processing operations; and

- have documentation ready which demonstrates to data subjects and to supervisory authorities the measures that have been taken to achieve compliance with the data protection rules." [79]

It is a standard rule that the usefulness of the measures should be checked regularly. There are several ways to assess the adopted measures and their effectiveness: monitoring, audits or data protection impact assessment. Therefore, the decision of using documentation may not be final at all.

Also, using documentation as an appropriate measure does not exclude using other measures. Resort may be made to documentation together with other measures, or as to additional legal tool.

Place of documentation in the compliance field is explicitly stated in Art 24.2:

"Where proportionate in relation to processing activities, the measures referred to in paragraph 1 (para above) shall include the implementation of appropriate data protection policies by the controller". [80]

The Regulation does not oblige controller to write this or that particular data protection policy. Again, the burden of assessment lies on the company itself – what measure it shall undertake and whether documentation would be such a measure is up to the company.

However, the Regulation provides that in certain circumstances, documentation may be appropriate.

In the view of the author, a company should assess whether to resort to documentation or not given the following issues:

1. If some information shall be sent without undue delay to another subject it is advisable to prepare a typical template.

2. If the company deems it desirable to describe how employees should treat personal data – policy as an internal document is recommended.

---

[79] Article 29 Working Party, Opinion 3/2010 on the principle of accountability

[80] GDPR, Art. 24(2)

3. If provision contains an obligation to keep some information – creating and keeping register is the best organisational way to comply.

Demonstration of compliance

Compliance with the GDPR – a significant issue, and so the demonstration of compliance is. The company should assure authorities that it complies with the GDPR with every part of its business activities.

Examples of demonstration of compliance linked with documentation are the following:

- records of consent ("the controller shall be able to demonstrate that the data subject has consented to the processing of his personal data"[81]);
- register of data breaches ("the controller shall document any personal data breaches");[82]
- records of the processing activities;
- existing of the necessity of processing personal data for the performance of a contract (Art.7.2) or legitimate interest (company should provide reasoning of such necessity of collecting personal data for contractual purposes. Such necessity is a condition for using a lawful basis);
- existing of automated decision-making and its role in data processing: "if a company use techniques such as artificial intelligence and machine learning to make decisions about people, in some instances, individuals have the right to hold the company to account by requesting explanations of those decisions and contesting them." [83]

Apart from the demonstration of compliance, there is a duty of the controller to cooperate with the supervisory authority, on request, in the performance of its tasks (Article 31 of the GDPR). Obligation to cooperate is also mentioned in Recital 82 providing that records of processing activities should be handed to authority on request.

Accountability is not just about reporting to the regulator; the company should

---

[81] GDPR, Art. 7(1)
[82] Ibid, Art. 33(5)
[83] ICO, Accountability and governance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

also demonstrate compliance in its interaction with natural persons.

For example, there are data subject rights having basis in a demonstration of compliance requirement (and they form a part of compliance in general), such as:

- right to rectification;
- right to be informed.

Chapter I Concluding Remarks

In the 21-st century, personal data significantly increased in their commercial and social value. The General Data Protection Regulation was adopted in the name of assuring the level of data protection, required by a current situation, given that companies collect personal data for [almost] free, and sometimes do not bother to store personal data securely.

One of the ways to protect data is to impose respective obligations on public and private bodies, processing personal data. Such obligations are based on the accountability principle. This principle has two parts – compliance (adopting organisational and technical measures to protect data subject rights) and demonstration of compliance.

Both tasks have a variety of possible solutions. Documentation may be a suitable measure to comply if it correctly reflects obligations of compliance or demonstration of compliance.

Use of a particular document should be preceded by analysis, conducted by the company – whether a policy or register helps with compliance in a specific case. Article 25 of the Regulation plays an essential role in this analysis establishing and describing data protection by design and by default approaches.

CHAPTER II
LIFE-CYCLE OF PERSONAL DATA AND RELATED DOCUMENTATION

2.1 Collection stage

Prior to collecting data, the controller should choose an appropriate lawful basis – an objective explanation of its interest in personal data – whether for providing services, or performance of a contract or in the name of protection vital interests of the data subject.

Lawful basis for collecting personal data stated in Art.6 of the Regulation.

For academic purposes of this diploma, most interested only 2 of them – consent and contract – because other lawful bases heavily depend on existing specific circumstances (legal obligation or interest) and there re no need in documentation preparation.

"Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes[84];

2. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract".[85]

Therefore, this thesis will contain description of requirements for processing personal data with consent or contract because of the importance of lawfulness of the collection stage.

2.1.1 Consent

Probably, the most famous lawful basis for collecting is consent.

It explains by the simplicity of this form for a user – one "opt-in" or signing

[84] GDPR, Art. 6(1)(a)
[85] Ibid, Art 6(1)(b)

action – and he or she has consented to provide his or her personal data to the company.

Simplicity can be achieved only with meticulous preparations. Consent, with all its advantages, has many requirements. Violation only one entail a violation of a lawfulness principle, prescribed by Art. 5.1(a) of the Regulation.[86]

Regulation allowed to prepare a text of the consent, so data subject only have to make an affirmative action.

Data subject consent form – is a short text in plain language, which asks user - "would you allow us to get your e-mail for e-mail marketing".

Data subject consent form is not a significant document, and drafting is easy. However, consent requires much more than only drafted text.

Definition of consent, stated in Art.4(11) of the Regulation, fully described general requirements for processing personal data with consent.

"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;" [87]

It will be useful to disassemble this definition and explain every part of it.

So, consent shall be:

- "freely given" consent meaning making no barriers and terms for data subject to give his consent on an exchange on something. For example, limitation of using services because of not giving a consent – will be a violation of the "freely given consent" principle.

As explained in Recital 42 general understanding of "freely given", "consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".[88]

The balance between data subject and controller or processor

"Freely given" means balance between controller and data subject – meaning no leverages over data subject to force him to give the consent. It called "imbalance of

---

[86] GDPR, Art 5(1)(a)
[87] Ibid, Art. 4
[88] Working Party 29, Recital 42 to the General Data Protection Regulation

power". For example, employer and employee.

Recital 43 describes it like this:

"In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation".[89]

Possibility of existing imbalance of power does not mean obligatory refusal to choose consent as a lawful basis for the processing of personal data. However, the controller should consider risks and take precautions, meant in "freely given consent" principle.

Consent should be apart from a contract or any other document.

Art. 7.4 of the Regulation reads:

"When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract". [90]

The ICO explains it as follows: "consent should be unbundled from other terms and conditions (including giving separate granular consent options for different types of processing) wherever possible". [91]

Also, Art. 7.2 of the Regulation provides an appropriate way of providing consent in written form:

"If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

Any part of such a declaration which constitutes an infringement of this

---

89 Working Party 29, Recital 42 to the General Data Protection Regulation

90 GDPR, Art 7(4)

91 ICO, What is valid consent: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

Regulation shall not be binding."[92]

This is a powerful statement – consent should be clear and understandable; all the opposite cases will be a violation and shall be punished.

Article 7.2 of the Regulation refers to "freely given consent" principle only in its small element - "manner which is clearly distinguishable from the other matters".[93]

Recital 43 provides more details on why it is necessary to split up consent from other provisions:

"Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance." [94]

Consent as a legal act should be separate and explicit. Contract and consent as lawful bases cannot be bundled too.

Furthermore, the ICO provides an opinion (and I fully agree with it), that electronic consent should have an opt-in box for every purpose of processing (unless you cannot do it). "Data subject should not be forced to agree to all or nothing – they may want to consent to some things but not to others." [95]

Looking further, mixing consent with provisions of a contract could be a violation in future – in case of any alteration or termination of a contract. Every single action with contract definitely touched linked with contract consent.

Covering consent among provisions is a violation of the freely given principle.

Summary

Consent will be freely given if:

- Consent is a single act and document
- Data subject free to give his consent for processing personal data or not

---

[92] ICO, What is valid consent: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

[93] GDPR, Art. 7(2)

[94] Working Party 29, Recital 43 to the General Data Protection Regulation

[95] ICO, How should we obtain, record and manage consent: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/

- Controller or processor should not use his power to influence on the data subject

- Refusal to give consent should not entail negative consequences to him as user/customer.

- "specific and informed consent" provision setting on controller obligation of providing detailed information in the understandable form about data processing to the data subject.

Specific consent should promote understanding by data subject terms of consent and consequences of entitling company for processing his or her personal data. The data subject should be informed about the future of personal data, and be aware of his right to control this future.

According to Working Party 29` guideline on consent, "to comply with the element of 'specific' the controller must apply:

– Purpose specification as a safeguard against function creep;

– Granularity in consent requests;

– Clear separation of information related to obtaining consent for data processing activities from information about other matters".[96]

Informed consent means the right of the data subject for minimal awareness about data processing. Article 13.1 described a very minimum of information about consent:

“- the identity and the contact details of the controller and, where applicable, of the controller's representative;

- the contact details of the data protection officer, where applicable;

- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

- where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

- the recipients or categories of recipients of the personal data, if any;”[97]

[96] Article 29 Working Party Guidelines on consent under Regulation 2016/679, p. 11
[97] GDPR, Art. 13(1)

Art. 5.1(b) of the Regulation says, that "personal data shall be collected for specified, explicit and legitimate purposes". [98] Information about purposes of consent should reflect this provision too.

About additional information, WP29 believes that "at least the following information is required for obtaining valid consent:

- what (type of) data will be collected and used;

- the existence of the right to withdraw consent (according to Art. 7.3, the data subject shall be informed about this right prior to consent)" [99]

- "possible risks of data transfer due to the absence of an adequacy decision and of appropriate safeguards as described in Article 46." [100]

It will be reasonable to add to consent information about nature processing activities (what controller is going to do with personal data). Any more information would be useful; however, putting too much information into consent may be a barrier with clear understanding.

Providing information heavily depends on form consent – oral, written or electronic form – and should include specifics of the form.

However, despite the form of consent, the information should be provided in clear and plain language, making consent understandable for the average person.

- “unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action”[101]

A "clear affirmative act" means that “the data subject must have taken a deliberate action to consent to the particular processing.” [102]

Despite this provision is clear, companies have problems with giving to data subject an opportunity to express his wishes. The electronic form of consent should be described more detailed.

The data subject can express his wishes:

- in oral form;

---

[98] GDPR, Art 5(1)(b)
[99] Ibid, Art. 7(3)
[100] WP 29 Guidelines on consent, p. 13
[101] GDPR, Art. 4(11)
[102] Commission Staff Working Paper, Impact Assessment, Annex 2, p. 20

- in written form;
- by electronic means. [103]

The action of consent in written form could be made by signing the document of consent.

Most controversial for business form – is electronic, because data protection confronts established e-commerce and marketing practices. Namely, many websites have pre-ticking boxes with "I agree with terms of consent". Such pre-ticking existing only because of marketing conviction, that "extra clicks reducing sales".

However, pre-ticking boxes or any other "opt-out consent" (when websites think, that data subject give consent, because he or she did not decline to option to give consent) and any other "silent actions" are a direct violation of Recital 32:

"Silence, pre-ticked boxes or inactivity should not therefore constitute consent".[104]

An appropriate way of consenting is an "opt-in" action. Recital 32 providing such examples:

"This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data."[105]

The ICO provides more examples of opt-in consent:

- "choosing preference dashboard settings;
- responding to an email requesting consent;
- volunteering optional information for a specific purpose – e.g. filling optional fields in a form (combined with just-in-time notices) or dropping a business card into a box". [106]

Summary

[103] Working Party 29, Recital 32 to the General Data Protection Regulation
[104] Ibid
[105] Ibid
[106] ICO, How should we obtain, record and manage consent: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/

The data subject should make an action, which expresses his decision to allow the company to collect and process his personal data. "Opt-out" will be a violation.

It is hard to say, that such requirement is new – Directive 95/46 contained provision about "unambiguous indication of consent". GDPR broadened this definition, bearing in mind modern business practices and clearly indicates – what can or cannot be identified as an unambiguous indication of the data subject's wishes.

Such a requirement makes sense because data protection has a higher priority than marketing optimization. This simple fact, unfortunately, still is not a guiding principle in most cases, and only big fines have an impact on companies.

Also, pre-ticked boxes often considered as dark-pattern - when websites are manipulating users, fraudulently forcing him to make a purchase he initially did not want to. It is positive that dark-pattern mechanisms were banished officially in the name of privacy.

There are several provisions in Article 7 of the Regulation, which have been cited before and prescribing more requirements for drafting and management of consent as a document.

- Demonstration of consent:

Art. 7.1 of the Regulation establishes that:

“Where the processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.”[107]

It means that the controller should store the evidence of consent been given. It may be audio records for oral consent, archive records of written consents, and cloud or hard drive records for electronic form.

It does not matter – what kind of depository will be used. Most important – make it easily accessible for employees to use it to answer the request of the supervisory authority. Moreover, it should be update-friendly – so authorized person could amend or delete information without a bunch of technical actions.

It would be reasonable to create a register of consents and carefully fulfil,

[107] GDPR, Art. 7(1)

maintain and update it, so demonstration of consent would be without undue delay or violations.

- Right to withdraw consent

Art. 7.3. of the Regulation prescribed, "the data subject shall have the right to withdraw his or her consent at any time (…) It shall be as easy to withdraw as to give consent" [108]

Withdrawal of consent – is, apparently, a most challenging part of consent management for controllers. Unfortunately, most of the companies completely forgot about this data subject right. Moreover, the provision about "shall be as easy to withdraw as to give consent"[109], when one-two clicks gave consent – make thing more complicated.

It seems complicated because, at the beginning one-two clicks started the process, the company wanted and being prepared for this. On the contrary, one-two clicks, made for the withdrawal of clicks, should cause immediate cessation of collecting and processing personal data, allowed by this consent. Even worse scenario – when data subject gave several consents for different purposes – and withdrawal of consent should stop processing only on a particular purpose.

The author believes, that that management of withdrawing of consent should be carefully described in records management policy.

2.1.2 Contract

Second most popular lawful basis for processing personal data is a contract. Given the purposes of this diploma, analysis of a contract does not mean the preparation of a separate document. Provisions and opinions mentioned below serve as guidance for when a company decides to collect personal data **on contractual purposes.**

According to Art. 6.1(b) of the Regulation:

“Processing shall be lawful only if and to the extent that at least one of the following applies:

[108] GDPR, Art. 7(3)
[109] Ibid

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."[110]

The Guidelines of European Data Protection Board on contract as a lawful basis, described legal elements of such a contract for processing personal data.

Contract as a lawful basis shall be used only if:

1) Contract really exists and controller acting in good faith

Processing is necessary for the contract, not contract for processing. WP29 Opinion on legitimate interests explain this issue as follows:

"[contract as lawful basis] does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller".[111]

A company shall not seek to sign a contract only to gain access to personal data. First of all - commercial purposes, then – data processing.

If any obligations of data subject to enter into contract and provide personal data exist, controller, according to Art. 13.2(e), "shall provide information about such obligation, including possible consequences of failure to provide such data"[112]

2) Existing of necessity

The main conditions for the processing of personal data are:

"the processing in question must be objectively necessary for the performance of a contract with a data subject, or

the processing must be objectively necessary in order to take pre-contractual steps at the request of a data subject."[113]

Both conditions contain requirement of existing "objective necessity" due to contract. Likely, that it works conversely – without such necessity, the EDPB considers that "where processing is not in fact necessary for the performance of a contract, such

---

[110] GDPR, Art. 6(1)(b)

[111] Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), p. 16–17.

[112] GDPR, Art. 13(2)(e)

[113] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, p.7

processing can take place only if it relies on another appropriate legal basis."[114]

The controller shall conduct the assessment of what is 'necessary' and for the determination "the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal".[115]

A company shall determine: "the nature of provided by contract goods or services, exact rationale of the contract, essential elements of the contract, and mutual perspectives and expectations of the parties to the contract."[116]

Then, the controller shall objectively evaluate, whether personal data necessary for the contract, or not, and choose appropriate lawful basis.

3) Legal scope

Article 6.1(b) also requires that the contract should be in accordance with national laws, including contract law and provisions of labour law, consumer protection law, e-commerce law, etc.

Termination of contract

When lawful basis of the processing of personal data is the contract, in case of termination of the contract - "as a general rule, the processing of that data will no longer be necessary for the performance of that contract and thus the controller will need to stop processing". [117]

In the name of terminating the contract, the controller may use personal data with the contract as a lawful basis or collect new data under consent.

However, the controller may not change a lawful basis for already collected personal data. Article 29 Working Party says "Under the GDPR, it is not possible to swap between one lawful basis and another." [118]

Thus, such requirements put on every contract, containing or meaning collecting of personal data. There is no room for preliminary drafting. However,

---

[114] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, p.9

[115] EDPS Toolkit: Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data, page 5

[116] Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, p.10

[117] Ibid, p.11

[118] WP29 Guidelines on consent under Regulation 2016/679, p. 31

training with staff, especially of the legal department, should be conducted to provide the awareness – a contract may be used as a lawful basis, not in every case – but only when it necessary, and necessity can be proven.

2.1.3 Privacy notice

A privacy notice is not related to a lawful basis or collecting as processing activity. However, the obligation of providing privacy notice when personal data obtained allowed the author to put this document in the collection stage chapter.

A consumer must be aware of any actions with his personal data. It is required by transparency principle – "Transparent processing is about being clear, open and honest with people from the start about who you are, and how and why you use their personal data." [119]

How should an organisation provide such awareness?

- Provide private information **at the time** when personal data are obtained (art 13) (if company received personal data from an individual, despite it was directly or indirectly).

- If a company received data from another source - inform person within a reasonable period, but at the latest within one month (Art. 14).

- Try to be short and straightforward. Facebook`s privacy policy, with almost 6,000 words, is longer than the USA Constitution.

Content of the privacy notice

Article 13 explicitly listed categories of information to be provided where personal data are collected from the data subject.

This information can be classified as essential and optional information.

What is essential to include in privacy notice:

1. “The name and contact details of your company (and your joint controller, if you have one);

2. The purposes of the processing;

[119] ICO, Principle (a): Lawfulness, fairness and transparency: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

3. The lawful basis for the processing (one or more bases from Art. 6.1 of the GDPR);

4. The retention periods for the personal data;

5. The rights available to individuals (right for access, complaint, rectification, erasure, restriction, objection, and data portability, and right to withdraw consent)" [120]

What should be mentioned, if it is applicable to controller:

– "Name and contact details of your representative or data protection officer, if you have one

– Recipients of the personal data – any third party, who received from you personal data (describe organizations or it types, and reasons, why you need to transfer this data)

– Information about transfers of the personal data to third countries or international organizations (basis and purpose)

– The details of whether individuals are under a statutory or contractual obligation to provide the personal data (Should be told people if they are required by law, or under contract, to provide personal data to controller, and what will happen if they don't provide that data.)

– The details of the existence of automated decision-making, including profiling"[121] If a controller received personal data from a third party, the following shall be mentioned:

1. "The source of the personal data

2. The categories of personal data obtained"[122]

The most challenging part, in the author's opinion, is describing purposes of the processing. Transparency principle requires an explicit explanation of why the controller needs personal data. Also, such an explanation should not be vague. WP29 Guidelines on transparency provides examples, how purposes of processing should

[120] GDPR, Art. 13
[121] Ibid, Art. 13
[122] Idib, Art. 14

NOT be put in privacy notice:

"We may use your personal data to develop new services" [123] (as it is unclear what the "services" are or how the data will help develop them);

"We may use your personal data for research purposes" [124] (as it is unclear what kind of "research" this refers to);

"We may use your personal data to offer personalised services" [125] (as it is unclear what the "personalisation" entails).

Requirements to privacy notice:

1. **provided without any barriers or obstacles**

Recital 58 states that:

"The principle of transparency requires that any information addressed to the public or to the data subject be (...) easily accessible (...). Such information could be provided in electronic form, for example, when addressed to the public through a website".[126]

The ICO listed examples, how a controller may provide this information through a variety of media:

1. "Orally - face to face or when you speak to someone on the telephone (it's a good idea to document this).
2. In writing - printed media; printed adverts; forms, such as financial applications or job application forms.
3. Through signage - for example, an information poster in a public area.
4. Electronically - in text messages; on websites; in emails; in mobile apps." [127]

Logic on a variety of these examples is simple – data subject should perceive information by any means but in commonly used or affordable sources.

2. **plain language with concise sentences**

---

[123] Article 29 Working Party Guidelines on transparency under Regulation 2016/679
[124] Ibid
[125] Ibid
[126] Working Party 29, Recital 58 to the General Data Protection Regulation
[127] ICO, What methods can we use to provide private information: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

Recital 58 demands information to be understandable.

"The principle of transparency requires that any information addressed to the public or to the data subject be concise … easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used".[128]

As mentioned above, intentional (and unintentional, too) vagueness of language constitutes a violation of the Regulation.

Vagueness usually provided by "language qualifiers such as "may", "might", "some", "often" and "possible"". [129]

Further, more tips about writing – it should be:

"in the active instead of the passive form and excess nouns should be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology. Where the information is translated into one or more other languages, the data controller should ensure that all the translations are accurate and that the phraseology and syntax make sense in the second language(s)." [130]

Also, the style of writing should be simple, appropriate, and understandable for users. A privacy notice can be assessed on the average educational level of writing (it means, whether it was written for college graduates, or Ph.D., etc.).

New York Times did research and read more than 150 privacy policies of big technology and media companies. Almost all of them were written in hard to understand language, with a lot of legal jargon.

"To be successful in college, people need to understand texts with a score of 1300. People in the professions, like doctors and lawyers, should be able to understand materials with scores of 1440, while ninth-graders should understand texts that score above 1050 to be on track for college or a career by the time they graduate. Many privacy policies exceed these standards." [131]

In 2017 average score of privacy policies was 1400+ (as for professionals), with

---

[128] Working Party 29, Recital 58 to the General Data Protection Regulation

[129] Article 29 Working Party Guidelines on transparency under Regulation 2016/679

[130] Ibid

[131] The New York Times, *We read 150 Privacy Policies. They Were an Incomprehensible Disaster*: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

GDPR enacted – 1330 approximately, and in 2019 – 1265.

Providing privacy information for children, of course, needs carefulness and preparations and mainly plain and understandable text.

Summary

The importance of privacy notice lies in requirement "to provide a notice when personal data obtained".

The easiest and least expensive way is putting notice on the website – one-time effort to comply (yet, updating and reviewing should be undertaken too). Companies, both small and big, often use such a scenario.

The advantages of this scenario are a generalization of all information (if data processing activities of the company could be put into one general framework) and providing information for every single user, whose personal data can be lawfully collected.

Here is a danger – if any provision of notice, or notice at all, violates provisions of Regulation, legal claims could be sent from every single user. Such history happened with Google, who was fined for 50 mln of euro. One of the accusations was a lack of transparency and clarity in the privacy policy.

Therefore, the publishing of privacy policy shall be preceded by a meticulous preparation of every single Article, clause, and provision, and after this – assessment of compliance with requirements of the Regulation of privacy notice.

2.2 Usage stage

Use of personal data shall be transparent and lawful. To ensure the fulmillment of this obligation, Art. 30 established an obligation of keeping record of the processing activities.

Considering the fact that this record tightly linked with routine business practise (processing activity) with personal data concerned, records of processing activities strongly connected to use of personal data. Given that, the records of processing activities is put in subchapter about usage stage.

Apart from storing personal data, the controller has to write down and store

records of processing activities – metadata of every operation with personal data, trusted to a company.

A requirement of keeping records of the processing activities is stated in Art. 30:

“Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility.”[132]

There is no definition of processing activities. However, examples of processing activities are provided in Art. 4.2 as a definition of "processing":

- “collection, recording, organization;
- structuring, storage, adaptation or alteration;
- retrieval, consultation, use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination, restriction, erasure or destruction."[133]

The importance of these records is high. These records are serving as proof of compliance not only with Art. 30 but could be used as verification of compliance at all, so the company can prove to the supervisory authority that the controller fulfilled the other requirements of the GDPR.

Several recommendations on the recording of the activities from Art. 30:

- “The records shall be in writing, including in electronic form.”[134]
- “The controller or the processor and, where applicable, the controller’s or the processor’s representative, shall make the record available to the supervisory authority **on request**.”[135]
- Organisation employing fewer than 250 persons, have no obligation about recording processing activities (“unless processing data is sensible, or processing likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional (are more than just a one-off occurrence or something you rarely do))”.[136]

[132] GDPR, Art. 30(1)
[133] Ibid, Art. 4.2
[134] Ibid, Art. 30(3)
[135] Ibid, Art. 30(4)
[136] Ibid, Art. 30(5)

Pieces of advice from the ICO regarding preparation for documenting processing activities:

– "do information audits to find out what personal data your organisation holds;

– distribute questionnaires and talk to staff across the organisation to get a complete picture of your processing activities; and

– review your policies, procedures, contracts, and agreements to address areas such as retention, security, and data sharing."[137]

Content of records

If a company is a controller for the personal data, it processes, according to Art. 30, the company need to document the following:

1. "the name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer;
2. the purposes of the processing;
3. a description of the categories of data subjects and of the categories of personal data;
4. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
5. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
6. where possible, the envisaged time limits for erasure of the different categories of data;
7. where possible, a general description of the technical and organisational security measures referred to in Article 32(1)." [138]

"Each processor and, where applicable, the processor's representative shall

[137] ICO, Accountability and governance: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/?q=record

[138] GDPR, Art. 30

maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

1. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

2. the categories of processing carried out on behalf of each controller;

3. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

4. where possible, a general description of the technical and organisational security measures referred to in Article 32(1)."[139]

Records of processing activities should answer questions – why and where you collect the data, and their future in your hands.

Polish public entity was fined for violation of Art. 5.2 – because of shortcomings in the register of processing activities. Such indicate all data recipients, nor did it indicate the planned date of data deletion for certain processing activities.[140]

Additional content of the records

A controller may be not limited by Art. 30 and add more provisions. Additional content may consider business processes and specify data processing needs.

It could be:

1. Registering other types of information related to personal data;
2. Automated decision or profiling – related information;
3. The CNIL recommends to supplement records with details - "processing legal base, and, depending on the cases, legal outsourcing of the data transfer to another country, rights that apply to the processing, existence of an automated decision, data origins, *etc*".[141]

The main aim of the records is to give full information about every action.

---

[139] GDPR, Art. 30(2)
[140] EDPB, National News [about fines under GDPR]: https://edpb.europa.eu/news/national-news_en
[141] CNIL, Record of processing activities: https://www.cnil.fr/en/record-processing-activities

Importance of the records of processing activities stressed by the fact, that Regulation in Art. 30 fully describes the content of the records. It is a rare example when direct requirements on the content of the document exist.

2. Linking data to documentation

A controller can connect data or other information with related documentation.

For example, in category “lawful basis of collecting”, in case of consent, controller can link this category with a copy of the consent of data subject, stored by the controller.

Also, it can be linked to:

- data processing agreements;
- privacy notice` information;
- records of consent or personal data breaches;
- other documentation

Importance of records as a company document

Apart from compliance, records of processing activities could be used as an internal tool for:

- centralising data – to stop simultaneous existing packages of data;
- structuring data – for easy and quick access to data by categories – data subject, type of data, basis of the collection, etc.
- tracking data – monitoring of retention periods of data, so delete or anonymise data will be held on proper timings, etc.
- connecting data – linked data subject and his data with his consent (or contract), storing in cloud of company.
- Appointing responsible person – setting and tagging responsible for personal data processes employees, who will be responsible for maintaining of records of processing activities.
- registering access sessions– who and when accessed personal data, and other actions wit data (copy or alteration).

Records of processing activities can be deemed as register of data, processed by a company. Of course, this "title" required fulfilling, maintaining, updating, and

publicising in a specific manner.

Keeping a record of processing activities is a challenge; records must reflect the current situation about the processing of personal data. Thus, the controller should treat records of processing activities as a living document that is updated as and when necessary. This means that the company should conduct regular reviews of the processed information to ensure that documentation remains accurate and up to date.

CNIL recommendation on updating of records: "The record must be updated regularly, according to the functional and practical evolving of data processing. In practice, any change brought to the conditions of processing implementation for each processing subscribed to the record (new data collected, lengthen of the preservation time, new processing recipient, etc.) must be added to the record."[142]

Concluding Remarks

Every single company, at least once processes personal data. Nowadays, processing personal data transforms into additional business activity, for example, in marketing. Sometimes companies, primarily operating in IT-field, processing such an amount of personal data, that by access to the data they gain leverages over the market. Such power definitely should be limited.

One of such limitations is a record of processing activities AND access to the record of supervisory authority under request. By recording every action, done with personal data, a company understands that every action could be investigated. Only this provision improves the level of compliance amongst companies.

Furthermore, records may be used for internal purposes – as memory of its actions, so that authorized employees can easily find personal data case.

2.3 Retention stage

After collecting personal data, the controller shall store them.

This stage usually attracts less attention from companies, than collection. However, it requires more expenses, more documents, and more compliance processes that need to be established.

[142] CNIL, Record of processing activities: https://www.cnil.fr/en/record-processing-activities

Personal data, after collection, shall be systematized, kept up to date, protected, and finally erased. All of these – different processes, should be described considering the business purposes of the company.

2.3.1 Data retention principles

The main storage principles stated in Art. 5 of the GDPR:

- data minimization;
- storage limitation;
- accuracy;
- integrity and confidentiality.

Short briefs of these principles have to explain further documentation process regarding the implementation of these principles in documents for retention stage.

Storing personal data is an ongoing process, and, as every process in the GDPR compliance, is based on principles to be included in the main document – records management policy.

Data minimisation

Art. 5.1.c stated:

"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, but not simply stored;"[143]

Notwithstanding the fact, that this principle is more connected with the collection stage, it would be useful to consider data minimisation in companies' records policy. Firstly, these recommendations are useful for the storage stage too – as a guiding principle for any action with already gathered data (re-using, for example).

Secondly, clear understanding and implementing this principle help company with fixing possible mistakes, made in collecting or usage stage,

We have three parts of this principle – adequate, relevant, and limited. All of them are sort of similar in context, yet all of them require not such a similar approach.

[143] GDPR, Art. 5(1)(c)

"Relevant data" provision directly connected with the purpose for collecting and using personal data. If a company collected it for one-time marketing action – it shall not dare to use it again and again.

Also, a company shall be careful with transferring of personal data among departments. Why they need it? For what purpose?

"Limited data" is close to "relevant data". While the second means the quality of information, "limited data" - a quantity of information (yet they have similar criteria to be assessed).

What does the company need from the consumer in store? Contact details – e-mail, address, phone. If company wants to keep him in touch with sales and discount news, company has no need for his or her health data, despite the fact that it could help to offer appropriate goods.

"Adequate data" says about turning to a general understanding of data processing. Indeed, a game app does not need access to a person's contacts.

The GDPR-makers seem to like turning to a general, not legal understanding of legal processes. In this matter, the company's compliance officers should think globally and try to answer questions like, "do we really need this data?"

The ICO for better implementation of this principle recommends:

- "only collects personal data you actually need for your specified purposes;
- have sufficient personal data to fulfill those purposes properly;
- periodically review the data you hold if it still relevant and adequate for your purposes, and delete any you do not need" [144]

Storage limitation

As written in Art. 5.1.e, "personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."[145]

Thus, the second part of the provision states: "kept no longer than is necessary".

Again, the burden of assessment is on a company: how long data should be

[144] ICO, Principle (c): Data Minimisation: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

[145] GDPR, Art. 5(1)

stored is up to the company. However, there is one strict criterion – the necessity of the retention period.

Such necessity is directly linked to collecting purposes and, of course, general evaluation of situation – controller has no need to store e-mail for 15 years.

However, in terms of storage periods, the controller shall comply not only with the GDPR but also with national law. Retention periods are spread all over the legislation of controller's country, and it is a challenge to find them all – retention periods, for example, of medical records, contracts, projects of buildings, etc.

Finally, what should be considered for complying with storage limitation principle:

– "to what extent they need to keep a record of a relationship with an individual once that relationship ends,

– to what extent they need to keep information to defend themselves from possible future legal claims, industry standards and guidelines, and any legal or regulatory requirements".[146]

The ICO and other reliable sources hold the opinion, that "personal data held for too long will, by definition, be unnecessary"[147]. By deleting or anonymizing personal data, controller no longer needs, company: 1) reducing expenses on data storage[148]; 2) reducing risks of data become inaccurate, irrelevant, out of date; and 3) get rid of obligation to maintain and update such personal data.

"Shall be kept in a form which permits identification of data subjects"[149] means personal data as it is. Anonymized data will not permit to identify person, so it describes a way to avoid this principle.

Accuracy

---

[146] Lydia F de la Torre, *What does "storage limitation" means under EU Data Protection Law*: https://medium.com/golden-data/what-does-storage-limitation-mean-under-eu-data-protection-law-fc6459ecb26c

[147] ICO, Principle (e): Storage limitation: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

[148] Expenses on data storage means any costs, paid for storage an amount of information, with applying organisational and security measures on data, stored by the company. According to Art. 25 of the GDPR, controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data that are necessary for each specific purpose of the processing are processed. That obligation applies to ... the period of their storage and their accessibility.

[149] GDPR, Art. 5(1)(e)

This principle is established by Art. 5.1.(d):

“accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.” [150]

This principle is essential for managing an appropriate updating of personal data, already collected from data subject.

First of all, this principle is cognate to data subject rights. Indeed, the obligation "kept up to date, erased or rectified without delay" is similar to rights of data subject on rectification and erasure, established by Chapter 3 of the Regulation.

However, accuracy principle requires controller to act preventively updating or erasing data not as the fulfilment of request but as data storage policy.

Inaccuracy

“Inaccurate data” has no definition in the Regulation; however, Article 5.1(d) hints, what makes data accurate – “considering processing purposes kept up to date and to real situation information about data subject”.[151]

Data Protection Act (data protection law of Great Britain) defines “inaccurate data” as information that incorrect or misleading as to any matter of fact.[152]

In the opinion of the author, the inaccuracy of data, among other things, should be assessed by the controller itself.

Kept up to date

Kept up to date personal data is vital for data processing as an ongoing business process. For example, if a company uses the address for delivery, which was given five years ago, a package may be delivered to a wrong person. Especially it concerns profiling – a company should not advertise balls because a person liked it 2 years ago.

Thus, updating personal data is useful for controller too.

Updating should consider a collecting purpose, usage rate, amount of data, and a category of data. Most important, in the author’s opinion, is a usage rate because frequency increases the risk of using inaccurate data.

---

150 Ibid, Art. 5(1)(d)
151 Ibid
152 Data Protection Act 2018, Art. 205(1)

Also, there is a sensitive issue of asking data subject to update information about him or her. The controller had better set a timing for such requests or find out the way to ask data subject in the least bothering manner. For this purpose, the controller should have contact details for communicating with data subject.

There is no even general advice for timings of updating personal data. Perhaps, it should be annual or biannual update of the whole filing system, with obligatory review in case of use of personal data, collected a year ago and have not been used since.

Erasing

Erasing as a part of the accuracy principle is in a sort of cooperation with the storage limitation principle, which states that "personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary". Thus, erasing is to be conducted when personal data is no longer necessary.

The procedure of erasing is to be described in a retention policy, in particular, what controller shall do when the retention period expires: delete data or anonymise (using what anonymisation techniques).

Even more relevant document is a retention schedule, which establishes: trigger action (what caused the start of the retention period – for example, signing of the contract with an employee); retention periods (how long data should be stored) and final action – review, deleting or anonymisation.

Such parameters should be unique for every category of personal data, ever collected by the company. Of course, controller set retention period, trigger action and final action on his own – Regulation have no specification on this matters.

Summary

Accuracy principle requires organisational and technical abilities – to update, erase, or rectify personal data. It leads to the main point of this principle – personal data must be structured in a manner, which permits such alterations without significant efforts.

Accuracy principle is an essential part of privacy by design. Controller should create a filing system, considering mid- and long-term needs – a high probability of

existing a necessity in updating or deleting personal data. Controller shall be prepared to handle dozens, hundreds, or dozens of hundreds of data subjects' requests. Such an approach concerns most of the processes – that company should build a system in a way that will help with the GDPR compliance by the lower costs.

Integrity and confidentiality (or Security) principle

This principle is set by Art. 5.1(f):

"personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"[153]

At the first page of the first chapter it is mentioned that 3 of the five most significant data breaches were caused by poor security.

Personal data shall be stored securely or never stored at all.

The ICO precisely described the primary goal of the security principle in its explanation of the security principle: "- The data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);

- the data you hold is accurate and complete in relation to why you are processing it; and

- the data remains accessible and usable, i.e., if personal data is accidentally lost, altered, or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned. "[154]

Security principle has two parts – technical and organisational measures.

Technical measures

Such measures can be differentiated to:

1) cybersecurity (against external unlawful access to data)

2) corporate security (against internal unlawful access to data (e.g. employees, who tried to access to data, they have no competency)

---

[153] GDPR, Art. 5(1)(f)

[154] ICO, Security: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

3) pseudonymisation of personal data.

It is hard to advise with a certain degree of appropriateness technical measures, and it is impossible to advise a one-size-fits-all measure.

Before choosing technical measures, evaluation of business processes should be made – why collect personal data, how, who and why will use it in the company, how data will be stored, and who shall be responsible for storing, etc.

Expenses for security will be lower than possible fine.

Organisational measures are:

– Restricting access to personal data. Access should be given: on a permanent basis – according to duties of employee; to other information – under request, on a one-time basis. Information should not be accessible by any employee at any time.

– Records of activities. It is useful to automatically record when employee uses his access to personal data, what personal data was copied or used as an attachment to latter, how data was altered, and on what grounds, etc.

– Providing awareness amongst staff.

Summary

Ensuring the security of personal data is an ongoing process, with much work to be done. Therefore, security policy has to be carefully complied with by the company and its employees in every routine operation with personal data.

Every principle of data storage has layered elements, all of them containing specific requirements.

It is useful to dissemble such requirements and examine it.

As was mentioned, case-law under the GDPR already established in its framework – companies being accused not in "violation of storage obligations", but in violation of specific clause, which applies to the whole process – transparency, accuracy, clarity, etc.

Some principles apply to the whole set of data processing activities, in particular principles of lawfulness, transparency, plain language. Other principles, however, mainly provided for data storage.

Given that the life-cycle of personal data storage stage is years and that the

value of personal data has an unstoppable raise – storage is more critical, that is considered now.

The principal document, governing storage stage, is a records management policy.

2.3.2 Records management policy

The main objective of this policy – to describe in detail every single process, which needed to be done or possibly should be done with stored personal data.

These processes are:

1. creating filing system;

2. filling it;

3. updating and changing it;

4. responding to data subject's requests (because such requests, on the basis of data subject's rights, always linked to already collected personal data);

5. erasing personal data, *etc.*

Records management policy should contain:

1. **Scope and application**

Scope: all personal data collected, all registers or records containing personal data or related information.

Application: data subjects, competent staff, compliance officers, other staff.

2. **Creating**

Usually, records or registers exist in written or electronic form (only records of consent could be in oral form).

In creation stage, long-term aim of every record or register should be:

3. **Easy and quick demonstration of compliance** – providing records to supervisory authority, or responding to data subject's request.

4. **Easy and quick access to personal** data and related information by company staff.

If a company does not adopt a data subject request policy, the record management policy will best suit to describe how to answer the request of the data

subject. It is the most relevant policy because responding to the request is closely related to already collected personal data.

5. **Secure storing of personal data** – practical implementation of organisational and technical measures to ensure an appropriate level of security – back-ups, access role-based restrictions.

6. **Fulfilling**

Company should appoint a competent person – Records manager – responsible for inputting personal data in systematized manner into records or registers.

7. **Review and alteration**

Records manager should be responsible for updates of personal data according to the "kept up to date" principle and conduct changes in the information about the subject.

Also, according to data subject's requests, a company should alter or erase information in his file.

This policy should describe the processes of collecting data and storing it in the depositories of the company. For this reason, it is especially challenging to choose a set of provisions, which at least roughly fit all companies.

Chapter II Concluding Remarks

In adopting documentation concerning processing activities as a compliance measure, a company has to consider not only content of a document, but related provisions.

These provisions may be called "characteristics" of a document. Those may include the following:

1. **timing issues** – when the document should be provided or in which cases the document is related to long-term actions;

2. **common practice** – publishing privacy notice is the easiest way to provide it; using opt-in mechanisms for consent, *etc.*;

3. **"indirect" provisions** – provisions of the Regulation indirectly imposing obligations on a company. As an example may serve the right of the data subject to be

informed when data subject sends a request to the company to find out the amount of his personal data collected by the company.

The obligation of the company to answer this request corresponds to this right. Therefore, such “indirect” obligation should by systematized and prescribed in the relevant policy.

Such “characteristics” of the documents are absolutely necessary. They should be considered and evaluated in the process of adoption of the documentation as a measure to comply with the Regulation.

Also, the complexity of consent as a legal instrument is worth mentioning. Many direct and indirect clauses and their full meaning, combined, making consent not so easy for using as a lawful basis.

CHAPTER III
CORPORATE DATA PROTECTION DOCUMENTATION

3.1 Corporate policies

3.1.1 Data protection policy

Data protection policy – one of the most known documents for GDPR compliance, highly hyped by tech-media in publications about privacy and "free template-generators" websites. In their opinion, privacy policy and data protection are enough to be GDPR-complied.

It is far from the truth, and this policy is definitely not a panacea. However, it has a unique role in compliance processes. So, what this policy actually is?

Data protection policy is a framework of data protection compliance of the company, guiding provisions for its staff.

The main objective of the policy – to serve as a public statement about high corporate standards of the company. A significant part of these standards – principles of the GDPR, understood and accepted as guidance.

Several provisions of data protection policy are intersecting in text or context provisions of other policies or documents. For example, retention principles form a part of the records management policy.

However, describing principles of data protection may be useful as a statement of how the company implements them in its routine data processing activities.

Data protection policy should be set out as a possible future of data for awareness of users/clients. Meaning, it shall cover questions of the access of third parties to personal data, especially – third parties outside the EEA and Privacy Shield.

What data protection policy may include?

1. Categories of personal data: collected data (if possible – with a list of often collected types of data); sensitive data; previously collected data.

2. Categories of data subjects (clients or consumers, website users, employees, children, etc.)[155]

[155] HM Insights, How to write your organisation`s Data Protection Policy – Top 10 tips:

3. Purposes of collecting. A data subject should be aware of why his or her personal data is being collected.[156]

4. Principles. Controller, apart from listing the principles, should try to explain how specifically the company implements those.

The principles listed in Art. 5 of the Regulation are the following:

"lawfulness, fairness, and transparency

purpose limitation

data minimisation

accuracy

storage limitation

integrity and confidentiality (security)

accountability".[157]

5. Data subject rights.[158] Data subject's rights are set out in chapter 3 of the Regulation: the right to access, right to rectification, right to erasure, right to data portability, right to object.

In the author's opinion, providing data subjects with information about their rights is never superfluous.

Process of responding to the request of a data subject (providing information, altering or deleting it) should be described in Data subject request policy or in Records management policy. Data protection policy only offers awareness on data subject rights and the ways for the realisation thereof.

6. Retention period[159]. Although this part will be covered by records management policy and in retention schedule, it is recommended: 1) to ensure that users know about the use of their data by a controller or anyone else; 2) to assure users that the data are being well secured; 3) to prescribe that no one has unlawful access to

---

https://www.harpermacleod.co.uk/hm-insights/2017/april/how-to-write-your-organisations-data-protection-policy-top-10-tips/

[156] Paul Newham, How To Quickly Write GDOR Policy Documents: https://red-robot.net/gdpr-policy/

[157] GDPR, Art. 5.1

[158] White Fuse, Sample Data Protection Policy Template: https://iapp.org/resources/article/sample-data-protection-policy-template-2/

[159] PrivacyPolicies, How to Build a GDPR Data Protection Policy: https://www.privacypolicies.com/blog/gdpr-data-protection-policy/

data.

7. Third party's cooperation[160] – processors and cross-border. Controller should establish a way of cooperation with processors, with essential describing of processing activities, to be carried out by processor,

8. Responsibilities of departments.[161]

To sum it up, data protection policy is essential as a statement of company`s compliance with the GDPR. In the era of media, sometimes it is crucial to make such a statement – if not for compliance, then for business reputation.

Unfortunately, most of the companies are missing some principles or misinterpreting them. Understanding the foundations of the GDPR is a sign that company is reliable enough to be trusted with the processing of personal data.

As an internal document, data protection policy sets guiding principles of data protection law, which should be an essential part of day-to-day processing activities. Yet, there is room for specifications, for example of the role of personal data in business activities of the company, ongoing and future projects.

3.1.2 Data breach policy

Data breach policy serves to establish correct response to a data breach: from detecting to documenting it.

There is no responsibility for a data breach at all (for example, for hacking). However, there is a responsibility for bad security or not conducting mandatory actions.

Data breach policy may contain the following provisions:

- designating competent employees and their duties in case of a data breach;
- notification of the supervisory authority and/or data subject, in particular, when a company must do it and what information shall be provided;
- measures to be taken to mitigate damage to a person's privacy;
- documentation of data breaches.

[160] European Diisocyanates and Polyols Producers Association, Data Protection Policy: https://www.isopa.org/gdpr-and-data-protection/

[161] PrivacyPolicies, How to build a GDPR Data Protection Policy: https://www.privacypolicies.com/blog/gdpr-data-protection-policy/

According to Art. 4.12 of the Regulation, '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."[162]

Unlawful use of personal data is an emergency for every company; therefore, its response shall be immediate. However, without preparation (which shall also include drafting of data breach policy), it is almost impossible to fulfil all obligations given the time pressure.

Preparations

The first step is drafting a data breach policy. The second – establishing a team responsible for reacting to a data breach (for example, Data response team).

This team shall include employees from different departments: at least from IT, Legal, and PR (Data Protection Officer, if necessary). This team should raise awareness amongst other employees about their reaction to a data breach (*e.g.,* issues of internal communication), as well as promote respect for personal data.[163]

Establishing such a team is crucial. Appointing a competent person when a data breach has already happened would slow down the processes (even if we assume that the person has enough of knowledge).

In case of a data breach, this team should:

1. report a data breach to top management;
2. conduct an investigation and determine the source and scope of a data breach, affected people, the severity of risks to the privacy of people;
3. identify appropriate organisational and technical measures to mitigate damage from a data breach; take these measures;
4. determine the necessity of sending data breach notification to the supervisory authority and, separately, to a data subject; and further send notification.[164]

Data breach notification is a message from the controller to the supervisory

[162] GDPR, Art.4(12)

[163] EUGDPR Academy, 5 steps to handle a data breach according to GDPR: https://advisera.com/eugdpracademy/knowledgebase/5-steps-to-handle-a-data-breach-according-to-gdpr/

[164] EUGDPR Academy, 5 steps to handle a data breach according to GDPR: https://advisera.com/eugdpracademy/knowledgebase/5-steps-to-handle-a-data-breach-according-to-gdpr/

authority and data subject in case of data breach required by the Regulation.

This document may not be drafted with a one-size-fits-all approach – text of the notification shall be different for every single case.

However, the obligation to send the notification without undue delay requires a company to draft it, to know what information to provide, and how to do it.

According to Art. 33 and 34 of the Regulation, in the case of a personal data breach:

"the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55;"[165]

"The processor shall notify the controller without undue delay after becoming aware of a personal data breach."[166]

"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."[167]

The Regulation draws attention to the importance of immediate public reaction to a data breach. Indeed, unveiling data breach case with its reasons and consequences for data subjects will promote the carefulness of a company with regard to future possibilities and risks of data breaches. Recital 85 stated that “one of the purposes of notification is limiting damage to individuals.”[168]

However, data breach notification is not mandatory in particular situations.

It is not required to send a notification to:

– supervisory authority - "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons";[169]

– data subject – "if controller takes measures to compromised personal data" OR "if high risk to the rights and freedoms of data subjects referred to in paragraph 1

[165] GDPR, Art. 33(1)
[166] Ibid, Art. 33(2)
[167] Ibid, Art. 34(1)
[168] Working Party 29, Recital 85 to the General Data Protection Regulation
[169] GDPR, Art. 33(1)

is no longer likely to materialise".[170]

The minimum requirements for the content of notification are described in Art. 33.3 of the Regulation:

"The notification referred to in paragraph 1 shall at least:

– describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

– communicate the name and contact details of the data protection officer or another contact point where more information can be obtained;

– describe the likely consequences of the personal data breach;

– describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."[171]

In the author's opinion, the requirements, if fulfilled, ensure that the supervisory authority and data subject receive enough information.

Another point is that the nature of personal data breaches demands immediate system checks, especially as regards sources of a breach.

"Measures taken or proposed to be taken (...) to mitigate its possible adverse effects" is, perhaps, the easiest part for drafting breach notification policy, if such measures were established in data breach policy.

A possible consequence of the breach is a much more complicated issue. Thus, after spotting sources of the breach, the next step is evaluating damages. It requires a comprehensive analysis of the situation, in particular, who was affected by the data breach and the level to which it influenced a data subject.

All in all, for evaluation, assessment and other steps the controller has about 72 hours. However, the time may be extended if the controller explains the reasons for the delay.[172] Therefore, the company would have more time to conduct all necessary actions.

---

[170] GDPR, Art. 34(3)
[171] Ibid, Art. 33(3)
[172] GDPR, Art. 33(1)

Risk to person's rights and freedoms

The requirement to send notifications to a supervisory authority and to a data subject have the same trigger - high risk to the privacy of data subjects.

Such a risks are described in Recital 75:

"The risk to the rights and freedoms of natural persons, varying likelihood and severity, may result from personal data processing which could lead to physical, material, or non-material damage, in particular:

1.where the processing may give rise to discrimination,

2.identity theft or fraud,

3.financial loss,

4.damage to the reputation,

5.loss of confidentiality of personal data protected by professional secrecy, etc."[173]

Measures to be taken

According to Recital 87, first of all, the company does whatever it has to to ascertain whether data breach happened or not. [174]

After this, the controller shall notify supervisory authority about the **"**measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects."[175]

Evidently, between these two stages, the controller may take the abovementioned organisational and technical measures. To determine which measures will be appropriate, the controller shall duly investigate data breach case.

The assessment of existing risk shall be an integral part of data breach processes (as mentioned above, the high risk to the rights and freedoms of natural persons is a trigger for sending notifications to supervisory authority and data subject).

Evidently, a data breach could cause damage in so many aspects of a person's life, that it is impossible to foresee universal measures. That is why the Regulation uses the assessment approach, defined above, according to which the company has a

[173] Working Party 29, Recital 75 to the General Data Protection Regulation
[174] Working Party 29, Recital 87 to the General Data Protection Regulation
[175] GDPR, Art. 34(3)(d)

competency to choose measures to be taken in a particular case.

According to Recital 76:

“The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context, and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk".[176]

Tips for assessing the risk are provided by the Guidelines on Personal data breach notifications:

– **Sensitivity of personal data** – if one of special categories of data, listed in Art. 9 of the GDPR was involved – the risk should be considered as high.

– **Ease of identification of individuals.** The company should assess - “how easy it will be for a party who has unlawful access to compromised personal data to identify specific individuals or match the data with other information to identify individuals. If data was encrypted, and a key to data was not breached – it can be argued that risk is low”. [177]

– **Severity of consequences**. Those significantly depend on the circumstances of data breach.[178]

The recommendations for a methodology of the assessment of severity of personal data breaches, issued by the European Union Agency for Network and Information Security, provide different scenarios of data breaches and, therefore, different consequences:

– **Loss of confidentiality**: the information is accessed by parties who are not authorized thereto or don't have a legitimate purpose of accessing;

– **Loss of integrity**: the original information is altered, and substitution of data can be prejudicial for the individual;

– **Loss of availability**: the original data cannot be accessed when necessary.

[176] Working Party 29, Recital 76 to the General Data Protection Regulation
[177] Working Party 29, Guidelines on Personal data breach notification under Regulation 2016/679
[178] Ibid

It can be either temporal or permanent (data cannot be recovered);

– **Malicious intent**: the breach was due to an error or mistake, either human or technical, or it was caused by an intentional act of malicious intent.[179]

Generally, these Recommendations contain similar advice for assessing the severity of data breach to the Guidelines of WP29. Thus, criteria for determining the severity of personal data breach are the following:

– data protection context (nature, scope of compromised personal data);

– ease of identification - how easily the identity of the individuals can be deduced from the data involved in the breach;[180]

– circumstances of data breach.

With the proper assessment of data breach, the controller shall choose and implement appropriate organisational or technical measures. Those should be directed to preventing possible data breaches (fixing security problems, conducting lections with staff, ordering secure data storage, etc.) and mitigating damages (compensation, or, if possible, agreement with third party about deleting personal data).

Documenting data breach

The Regulation rarely imposes an explicitly formulated obligation on the company.

However, according to Art. 33.5 of the GDPR:

“The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects, and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."[181]

In the author’s opinion, the controller should additionally record reasoning for not sending a notification to a data subject under Art. 34(3) of the GDPR, or for delayed notification.

---

[179] Recommendations for a methodology of the assessment of the severity of personal data breaches, issued by European Union Agency for Network and Information Security in December 2013, p.11

[180] Recommendations for a methodology of the assessment of the severity of personal data breaches, issued by European Union Agency for Network and Information Security in December 2013, p.9

[181] GDPR, Art. 33.5

Art. 33.5 of the Regulation rises the importance of risk assessment, described and explained above, even more. Therefore, the controller shall document 1) how data breach affected data subjects; 2) what measures had been taken, and why they were considered as appropriate.

Literally, the company should write this information two times – in data breach notification and in data breach register (filing system for documenting of data breaches). Guidelines on data breach notifications point out that "to show compliance with GDPR, it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches."[182]

Therefore, precedents should serve an educational role for staff, hence knowledge of level and details of data security certainly improves the preventing mechanisms for data breaches.

3.1.3 Employee data protection policy

A punishable situation in a company can be revealed through proactive inspection activities conducted by an unsatisfied employee.[183]

Employee data protection policy is an internal policy of a company, set to the regulate the turnover of personal data between employee and employer (controller).

Considering how close such a relationship is, the scope of this policy will cover more than any other. Indeed, with years and years of relations, a company makes a much more detailed profile about its employees, than about any other person. It happens, partly, due to the purpose of processing – special interest of a company in its employee, including medical or criminal aspects of his life.

Provisions of this policy are similar to data protection policy, with some specifications.

Data subjects – current and former employees or candidates. [184]

---

[182] Working Party 29, Guidelines on Personal data breach notification under Regulation 2016/679

[183] WP29, Fines/Penalties: https://gdpr-info.eu/issues/fines-penalties/

[184] City of London, Data Protection Policy (Employees): https://www.cityoflondon.gov.uk/about-the-city/access-to-information/Documents/employee-data-protection-policy.pdf

Material scope is larger because the definition of personal data is broadened with regard to employees.

The Regulation, providing a general explanation of personal data, reads as follows:

“in case law of the European Court of Justice recordings of work times which include information about the time when an employee begins and ends his workday, as well as breaks or times which do not fall in work time, [considers] as personal data."[185]

If a person can be theoretically identified, the following information may be regarded as personal data:

“written answers from a candidate during a test and any remarks from the examiner regarding these answers”;

“IP addresses (with additional information)”;[186]

Also, personal data may include:

“Subjective information such as opinions, judgements or estimates – for example, an assessment of the creditworthiness of a person or an estimate of work performance by an employer”;[187]

Such expansion of the definition of personal data entails widening of the scope of the Regulation over information, which may not be regarded by a non-lawyers as personal data. So, policy or corporate training should promote awareness amongst staff, especially in the HR department.

Furthermore, the employer is allowed (under certain circumstances) to collect special categories of personal data, listed in Art. 9.1 of the Regulation (genetic, biometric data, racial or ethnic origin, etc.).

According to Art. 9.2 of the GDPR, processing of special personal data shall be not prohibited, if:

“b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of

[185] WP29, Personal Data: https://gdpr-info.eu/issues/personal-data/
[186] Ibid
[187] Ibid

employment (...) or a collective agreement";[188]

"f) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee".[189]

The employee data protection policy shall also cover the processing of sensitive data, in particular, how to collect, how to process, how to store, and, the most important – criteria of the necessity of processing such sensitive data, and explanation and reasoning for the need in such processing.

Collection stage

An employer company should be careful in choosing a lawful basis for processing of personal data.

Consent, given by an employee, shall be free. Any pressure on an employee to receive his or her consent is prohibited.

For example, PWC Business Solutions was fined for 150.000 EUR. One of the infringements was, that PWC as a controller:

"has processed the personal data of its employees in an unfair and non-transparent manner contrary to the provisions of Article 5(1)(a) indent (b) and (c) of the GDPR giving them the false impression that it was processing their data under the legal basis of consent pursuant to Article 6(1)(a) of the GDPR, while in reality it was processing their data under a different legal basis about which the employees had never been informed."[190]

If a lawful basis is a contract, an employer should not collect all possible information about the employee – the company may collect only data, necessary for the performance of contract, or for the preparation thereof.

Summary

This policy is essential to be established and to provide a framework for the access and use of personal data of employees (including medical information, results of annual work performance tests, etc.). Other issues shall be regulated by general provisions of the GDPR, described in this diploma.

---

[188] GDPR, Art. 9(2)(b)
[189] Ibid, Art. 9(2)(f)
[190] EDPB, National News [about fines under GDPR]: https://edpb.europa.eu/news/national-news_en

Employee data protection policy is important, mostly because of the broadening of horizons of the "personal data" definition. Such broadening, in the majority of cases, is left beyond the attention of employers, and personal data of employees are often treated as ordinary information. Therefore, it is recommended to raise awareness among the departments of a company and to provide instruction on ways of treating information about work-time hours, work performance tests results, etc.

3.2 Other documents

3.2.1 Records of consent

According to Art. 7.1 of the Regulation, “controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data".[191]

It means that a controller should store the evidence confirming that the consent has been given by a data subject and demonstrate it by request.

The Regulation does not provide for the required or advised form of records. The form is heavily dependent on the form of consent given. Thus, it may be audio records for oral consent, archive records of written consents, and cloud or hard drive records for electronic form.

Records of consent should contain the following information[192]:

– **Who consented –** name of person, job or education additionally, or nickname of a user;

– **When they consented** – a time of clear affirmative action of consent;

– **What they were told at the time –** the most important point. For what purposes of processing he or she consented; consent was freely given and clearly indicated. Overall, this part serves as a demonstration of compliance with Article 6, 7 of the Regulation, and other provisions on consent as a lawful basis.

– **How they consented –** in oral, written or electronic form;

[191] GDPR, Art. 7(1)

[192] ICO, How should we obtain, record and manage consent: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/

– **Whether they have withdrawn consent –** if it happens, the company should record time of withdrawal and other related information**.**

Review of records

First of all, records should be reviewed, considering the timings of consent.[193]

Consent is usually given for some purpose. With time, this purpose is changing by itself: a person has another data, a company has other business processes.

Working Party 29 recommends that "consent should be refreshed at appropriate intervals. Providing all the information **again** helps to ensure the data subject remains well informed about how their data is being used and how to exercise their rights."[194]

Secondly – records of consent should be an integral part of data depository, so the withdrawal of consent puts an end to the collection of personal data.

Records of consent are an essential part of the demonstration of compliance, so text and metadata of consent should be carefully recorded and stored in a systematized and easy-to-access manner.

3.2.2 Data processing agreement

Data processing agreement is a contract between a controller and a processor when the processor is obliged to conduct processing activity on behalf of the controller. This activity can involve anything – collecting, storing, altering, etc.

According to Art. 28.3 of the Regulation, "processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller ."[195]

Conclusion of data processing agreement is required in two cases:

---

[193] ICO, How should we obtain, record and manage consent: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/

[194] WP29 Guidelines on consent, p. 21

[195] GDPR, Art. 28(3)

– when controller engages processor;[196]

– when processor engages another processor (sub-processor);[197]

In other words, such agreement is essential when another company conducts processing. That is why preliminary drafting and understanding of general principles of processing is highly important.

First, it should be clarified who is a controller or a processor:

"'**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."[198]

"'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[199]

There is practice when a Polish public entity was fined for PLN 40,000 for the infringement of Art. 28.3 of the Regulation. The mayor of the city had not concluded a data processing agreement with another public entity to which he transferred data.

Such transfer also violated the principle of lawfulness of processing stipulated in Art.5.1(a) and the principle of confidentiality provided for in Art.5.1(f) of the Regulation.

Recital 81 establishes key requirements that a processor should meet to process personal data: "To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing."[200]

Main requirements for data processing agreements stem from the security field.

Article 28.3 of the Regulation explicitly described clauses of the agreement and

[196] Ibid, Art. 28(3)
[197] Ibid
[198] GDPR, Art. 4(7)
[199] Ibid, Art. 4(8)
[200] Working Party 29, Recital 81 to the General Data Protection Regulation

corresponding obligations of a controller and a processor concerning personal data:

"That contract or other legal act shall stipulate, in particular, that the processor:

1. Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation (...) in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest"; [201]

The provision comprises two elements: documented instructions and obligation to inform.

Instructions to processor are extremely important, as the processor will undertake processing activity on behalf of the controller. Therefore, a company shall accurately describe categories and scope of personal data to be collected, as well manner of storage or any other processing activity.

2. "ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;"[202]

This clause corresponds to Art. 28.1 of the Regulation and integrity and confidentiality principles described above.

Art. 28.1 of the Regulation reads as follows:

"Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."[203]

It means that when a company conducts processing for another company, a controller is still responsible for the security of personal data. Furthermore, further provisions of Art. 28.3 of the Regulation pay a lot of attention to cooperation in the security field.

---

[201] GDPR, Art. 28(3)(a)
[202] Ibid, Art. 28(3)(b)
[203] GDPR, Art. 28(1)

3. “takes all measures required pursuant to Article 32;"[204]

Measures required in Art. 32 of the Regulation have to be undertaken with a previous assessment of the nature and scope of personal data, context, and purposes of the processing. Examples of such measures include:

– “the pseudonymisation and encryption of personal data;

– the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

– the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

– a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.”[205]

4. “respects the conditions referred to in paragraphs 2 and 4 for engaging another processor";[206]

Paragraph 2 stipulates, “the processor shall not engage another processor without prior specific or general written authorisation of the controller"[207]

Paragraph 4 states that sub-processor has the same data protection obligations for data processing activities as the processor.[208]

5. “taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures";[209]

6. “assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor";[210]

7. “makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute

[204] Ibid, Art. 28(1)(c)
[205] GDPR, Art. 32(1)
[206] Ibid, Art. 28(1)(d)
[207] Ibid, Art. 28(2)
[208] Ibid
[209] Ibid, Art. 28(1)(e)
[210] Ibid, Art. 28(3)(f)

to audits, including inspections, conducted by the controller or another auditor mandated by the controller."[211]

The Regulation requires the controller to ensure a proper level of security when engaging the processor. It includes both individual actions of the controller and his actions in cooperation with the processor – starting from the preliminary assessment of the reliability and fidelity of the processor up to the joint implementation of security measures.

So, data processing agreement should include:

– name of the controller and the processor, their contact details;

– description of the processing task – nature and approximate scope of personal data, type and scope of processing activities;

– process of transferring personal data to processor or time of beginning of processing activity;

– individual and common security obligations of both parties (including taking of measures and implementation of safeguards)

– sub-processor clauses – whether or not the controller allows the engagement of one;

– actions in case of data breach;

– other obligations of the processor (sending a notification about data breach or receiving data subject request).

Chapter III Concluding Remarks

According to Art. 25 of the Regulation, where proportionate, the controller shall adopt data protection policies.

The policies described in this Chapter may be considered among the most significant data protection policies.

A data protection policy is a public statement, which provides both general (“company abide with provisions of the Regulations in following”) and specific

[211] Ibid, Art. 28(3)(h)

information (how a company will communicate requests, based on data subject's rights).

A data breach policy is a comprehensive document, describing the response of a company to a data breach. It is especially important to know what to write in data breach notification and data breach policy.

The importance of the employee data protection policy lies with the fact, that a company collects more personal data from its employees than from the average person.

In conclusion, when adopting policies and other documents, it is advisable to know "characteristics" of the above documents, "indirect" provisions, timing issues (especially for data breach) and other questions.

CONCLUSIONS

The main conclusion of this thesis that documentation indeed may be an appropriate measure for the controller or processor to comply with provisions of the General Data Protection Regulation.

Following the principle of data protection by design and by default, the company shall assess a document before adopting it as an appropriate compliance measure. To ensure a required level of appropriateness of the specific document as a measure, a company in its assessment should consider the following:

Law. It is necessary to take into consideration relevant provisions of the Regulation and Recitals to it. Articles may contain both direct and indirect provisions, governing documentation.

Direct provisions set an obligation of the company with regard to adopting the document. (e.g., Article 30 - “controller shall maintain records of processing activities”).

Indirect provisions either generally apply to data protection or indicate the possibility of adopting a document (e.g., Article 30 - “controller shall provide information in privacy notice when personal data are obtained”).

Principles of processing, which apply to all processing activities, may serve as an example of general provisions. Nevertheless, such principles, as data minimisation, accuracy, storage limitation and integrity in combination require a special process of retention of personal data.

Purposes. A company is recommended to evaluate the benefit of document for accountability obligations of the company. The following are several purposes, different for every document:

1. to comply with provisions of the Regulation (fulfilment of obligations by the company);
2. to establish and describe a processing activity (storing personal data; analysis of information for drafting a data breach notification);

3. to prepare a document for a particular situation (privacy notice, which provides relevant information to the appointed data subject);

4. to record information (records and registers; recording data is significant enough to separate it from other processing activities).

One document may serve for more than one purpose.

Characteristics of the document include:

1. contents of the document;

2. time-related matters – timing for providing the document, or time for retention of personal data;

3. a common practice of drafting, providing or maintaing documents;

4. plain language requirement (for documents or information to be provided to the users, *i.e.* data breach notification, data protection policy).

Specific character of business. The company is recommended to consider its purposes and needs in data processing, and evaluate the scope of present and future processing activities. If some of the processing activities are periodic, systematic and significant in its scope – it is advisable to implement documentation.

Also, the specific character of business should be considered in choosing a lawful basis for the processing personal data and purposes of such processing because these provisions are directly linked with the lawfulness principle.

It is recommended to conduct a preliminary analysis before choosing documentation as an appropriate measure to comply with provisions of the Regulation and evaluating the possibility of choosing the document for adopting in data protection compliance. Only with the previous analysis documentation may be used as a measure to comply with the General Data Protection Regulation.

REFERENCE LIST

Primary sources

Law

1. Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950

2. Data Protection Act 2018

3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

4. 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

5. Article 29 Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017

6. Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, 3 October 2017

7. Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017

8. Article 29 Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010

9. Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), 9 April 2014

10. European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, 8 October 2019

11. European Data Protection Board, Guidelines 3/2018 of on the territorial scope of the GDPR (Article 3), 16 November 2018

12. Organisation for Economic Co-operation and Development (OECD),

Recommendation of the Council concerning Guidelines governing the protection of privacy and transborder flows of personal data

Court decisions

13. Ben Faiza v. France, no. 31446/12, 8 February 2018, ECtHR

14. Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v. Planet49 GmbH, C-673/17, CJEU

15. College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, C-553/07, CJEU

16. I v. Finland Application no. 20511/03, 17 July 2008, ECtHR

17. Malone v. United Kingdom, no. 8691/79, 2 August 1984, ECtHR

18. M.N. and Others v. San Marino, no. 28005/12, 26 April 2012, ECtHR

19. Patrick Breyer v. Bundesrepublik Deutschland, C-582/14 CJEU,

20. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, 27 June 2017, ECtHR

21. S. and Marper v. the United Kingdom [GC], Applications nos. 30562/04 and 30566/04, 4 December 2008, EctHR

22. Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság (C- 230/14) Judgement of the Court of Justice of the European Union

23. Z v. Finland, Application no. 22009/93, 25 February 1997, ECtHR\

Secondary Sources

24. Article 29 Working Party, *Personal Data*: https://gdpr-info.eu/issues/personal-data/

25. Article 29 Working Party, *Fines/Penalties*: https://gdpr-info.eu/issues/fines-penalties/

26. Center for Information Policy Leadership, "*Data Protection Accountability: The Essential Elements A Document for Discussion"*

27. City of London, *Data Protection Policy (Employees):* https://www.cityoflondon.gov.uk/about-the-city/access-to-information/Documents/employee-data-protection-policy.pdf

28. CNBC, *5 of the biggest data breaches ever*: https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html

29. CNIL, *Record of processing activities*: https://www.cnil.fr/en/record-processing-activities

30. Commission Staff, *Working Paper, Impact Assessment, Annex 2*

31. EDPB, *National News [about fines under GDPR*]: https://edpb.europa.eu/news/national-news_en

32. EDPS Toolkit: *Assessing the Necessity of Measures that limit the fundamental right to the protection of personal data*

33. EMC, *Executive Summary Data Growth, Business Opportunities, and the IT Imperatives*: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

34. EUGDPR Academy, *5 steps to handle a data breach according to GDPR*: https://advisera.com/eugdpracademy/knowledgebase/5-steps-to-handle-a-data-breach-according-to-gdpr/

35. European Union Agency for Network and Information Security, *Recommendations for a methodology of the assessment of the severity of personal data breaches*, December 2013

36. European Diisocyanates and Polyols Producers Association, *Data Protection Policy*: https://www.isopa.org/gdpr-and-data-protection/

37. HM Insights, *How to write your organisation`s Data Protection Policy – Top 10 tips*: https://www.harpermacleod.co.uk/hm-insights/2017/april/how-to-write-your-organisations-data-protection-policy-top-10-tips/

38. ICO, *Accountability and governance*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

39. ICO, Data protection by design and default: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

40. ICO, *Documentation*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

41. ICO, *How should we obtain, record and manage consent*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/

42. ICO, *Principle (a): Lawfulness, fairness and transparency*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

43. ICO, *Principle (c): Data Minimisation*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

44. ICO, *Principle (e): Storage limitation*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

45. ICO, *Security*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

46. ICO, *What is valid consent*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/

47. ICO, *What methods can we use to provide private information*: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/

48. International Conference of Data Protection and Privacy Commissioners, "*International Standards on the Protection of Personal Data and Privacy – The Madrid Resolution*"

49. Know Your Compliance, *How to Write a GDPR Data Protection Policy*: https://www.knowyourcompliance.com/how-to-write-a-gdpr-data-protection-policy/

50. LawScot, *Appendix 2 – Example of a data protection policy*: https://www.lawscot.org.uk/members/business-support/gdpr-general-data-protection-regulation/gdpr-guide/appendix-2-example-of-a-data-protection-policy/

51. Lydia F de la Torre, *What does "storage limitation" means under EU Data Protection Law*: https://medium.com/golden-data/what-does-storage-limitation-mean-under-eu-data-protection-law-fc6459ecb26c

52. Paul Newham, *How To Quickly Write GDOR Policy Documents*: https://red-robot.net/gdpr-policy/

53. PrivacyPolicies, How to Build a GDPR Data Protection Policy: https://www.privacypolicies.com/blog/gdpr-data-protection-policy/

54. Security Trails, *Top 5 Ways to Hande a Data Breach*: https://securitytrails.com/blog/top-5-ways-handle-data-breach

55. The New York Times, *We read 150 Privacy Policies. They Were an Incomprehensible Disaster*: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

56. THEVERGE, *Google fined €50 million for GDPR violation in France*: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

57. White Fuse, *Sample Data Protection Policy Template*: https://iapp.org/resources/article/sample-data-protection-policy-template-2/