Personal data protection: EU perspective (by Diana Javadyan)

Nowadays, more than ever, data protection issues are actual and crucial in terms of both data protection standard setting and data protection standard implementation. Recent Fintech developments, e-communities, artificial intelligence application and other technological advancements throughout the world bring up the need of robust data protection framework and protected data processing systems.

European Union (EU) has introduced the General Data Protection Regulation[1] (GDPR), which is applicable as of 25 May 2018. It creates a harmonized set of rules applicable to all personal data processing across EU. The objective of this new set of rules is to ensure that personal data enjoys a high standard of protection everywhere in the EU, increasing legal certainty for both individuals and organizations processing data, and offering a high degree of protection for individuals.

Personal data protection regulation: GDPR main highlights

What is personal data? Article 4 of the GDPR provides the definition of "personal data" which is any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is the one who can be identified by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The individuals are "identified" or "identifiable" if you can distinguish them from other individuals. A name is perhaps the most common means of identifying someone. However whether any potential identifier actually identifies an individual depends on the context. A combination of identifiers may be required to identify an individual. The GDPR provides a non-exhaustive list of identifiers such as name, identification number, location data and an online identifier. "Online identifiers" includes IP addresses and cookie identifiers, which may be personal data. Other factors also can identify an individual.[2]

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered more sensitive and may be processed only in limited circumstances.

The GDPR provides the core definitions applied in data protection framework, the main principles of personal data processing and collection, requirements for data processing and data protection standard setting, enforcement mechanisms for GDPR application.

The GDPR applies to "controllers" and "processors" operating in the EU. The controller defines the purposes and means of processing personal data. The processor is responsible for processing personal data on behalf of a controller. The GDPR applies to processing carried out by companies operating in the EU. However, it does not apply to certain activities such as processing covered by the Law Enforcement Directive or processing for national security purposes.

---

[1] 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), (see full text at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679)

[2] See at Guide to the General Data Protection Regulation (GDPR), Information Commissioner's office, August 2018, pages 10-11.

Seven principles of GDPR

GDPR sets out seven key principles, which lie at the heart of the general data protection framework. The principles are the following:

Lawfulness, fairness and transparency – it means that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation – it means that personal data shall be collected for specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with those purposes.

Data minimization - it means that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy - it means that personal data shall be accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified immediately.

Storage limitation- it means that personal data shall be kept in a form, which permits identification of data, subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Integrity and **confidentiality -** it means that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Compliance with the spirit of these key principles is therefore a fundamental building block for good data protection practice.

Violation of these principles may be subject to substantial administrative fines. GDPR states that infringements of the basic principles for processing personal data are subject to the highest administrative fines. This could mean a fine of up to €20 million, or 4% of companies' total worldwide annual turnover, whichever is higher.

Rights of data subject under GDPR

Individuals (data subjects) are entitled to certain rights under the GDPR. They have **the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling**.

Data subjects shall have the **right to be informed** about the collection and use of their personal data. This is a key transparency requirement under the GDPR. Processing company must provide individuals with information including purposes for processing of personal data, retention

periods for that personal data, who it will be shared with and other information related to data processing.

The right of access gives data subject the right to obtain a copy of their personal data, its undergoing processing as well as other additional information. It helps data subjects to understand how and why the controller is using their data, and verify if it is done lawfully.

Data subject shall have the right to obtain from the controller without undue delay the **rectification** of inaccurate personal data concerning him or her (right to rectification).

Data subjects shall have a **right to have their personal data erased (right to be forgotten)** in cases defined by laws. Particularly, if personal data is no longer necessary for the purpose for which it was originally collected or processed, the data subject may withdraw consent on which the processing is based. The data subject also may object to the processing of personal data if it has been unlawfully processed.

Data subject shall also have a **right to restriction of processing** in cases the data is not accurate in the opinion of data subject and its accuracy shall be verified by the controller.

The right to data portability gives data subjects the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request the controller to transmit this data directly to another controller. The right to data portability only applies when:

- the lawful basis for processing this information is the consent or for the performance of a contract;
- and the processing is carried out by automated means (i.e. excluding paper files).

Sometimes personal data a data subject has provided to controller will be easy to identify (e.g. username, mailing address, age). However, the meaning of data provided to the controller is not limited to this. It can involve personal data resulting from observation of an individual's activities (e.g. where using a device or service) such as history of website usage or search activities traffic and location data. The right to data portability may entitle data subject to receive a copy of their personal data; and/or have their personal data transmitted from one controller to another controller, where technically feasible. Although controllers are not required to use an interoperable format, it is encouraged to promote the concept of interoperability. An "interoperable format" is a type of format that allows data to be exchanged between different systems and be understandable to both.

When data processing is allowed?

Processing of personal data is allowed if there are valid grounds for that. This is called a "lawful basis" for processing and there are six options that are considered valid, particularly:

Consent: the individual has given clear consent for the company to process their personal data for a specific purpose.

Contract: the processing is required under a contract the company has entered into with the data subject, or processing is required to take specific steps before entering into a contract.

Legal obligation: the processing is necessary for the company to comply with the law (not including contractual obligations).

Vital interests: the processing is necessary to protect the vital interests of data subject.

Public interest: the processing is necessary for the company to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
Legitimate interests: the processing is necessary for company's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if the company is a public authority processing data to perform its official tasks.)[3]

There are many discussions on when the consent is considered valid. It must be freely given, specific, informed and must indicate data subject's approval by a statement or by a clear affirmative action to process personal data related to data subject. As a general rule, if data subject has no real choice, feels compelled to consent or will bear negative consequences if they do not consent, then the consent will not be valid.

Requirements towards data controllers and processors

GDPR also sets certain standards towards controllers and processors. The controller shall implement technical and organizational measures, such as pseudonymization and data minimization, to demonstrate that processing is performed in accordance with GDPR. Those measures shall be reviewed and updated. The controller shall use only processors providing sufficient guarantees for the protection of the rights of the data subject.

Processing by processor shall be governed by a contract or other legal act under Union or Member State law which is binding on the processor with regard to the controller and which 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. Each controller shall maintain a record of processing activities under its responsibility.

As to security standards, the controller and the processor shall implement technical and organizational measures to ensure the security of processing by means of pseudonymization and encryption of personal data, ensuring 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. They shall set up a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for security of the processing.

Data protection impact assessment

An interesting tool introduced by GDPR is the data protection impact assessment. The controllers will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals. Use of innovative technologies, use of profiling or special category data to decide on access to services, profile individuals on a large scale, processing of biometric or genetic data by controller may be considered as a high risk and require impact assessment by the controller. The data protection supervisory authorities shall establish and make public a list of processing operations that are subject to data protection impact assessment. It shall contain at least a description of the certain processing operations and the purposes of the processing, an assessment of the necessity and proportionality of the processing operations, an assessment of the risks to the rights and freedoms of data subjects and the measures to address and

[3] See at Guide to the General Data Protection Regulation (GDPR), Information Commissioner's office, August 2018, page 20.

mitigate the risks, including safeguards and security measures. A data protection officer, responsible for data protection, will be designated by public authorities and by businesses, which process data on a large scale.

Data transfers outside EU

GDPR also applies to international data transfers that is personal data transfers to third countries or international organizations. A transfer of personal data to a third country or an international organization may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. In this regard, European Commission adopts adequacy decisions for data transfers to third countries. The framework of adequacy decisions was impacted recently by the Court of Justice of the European Union (CJEU) Schrems II judgement. Particularly, in its July 2020 Schrems II judgment[4] the CJEU declared the European Commission's Privacy Shield Decision invalid on account of invasive US surveillance programs, thereby making transfers of personal data on the basis of the Privacy Shield Decision illegal. The Privacy Shield framework provides for the possibility of lawful transfer of personal data from the EU to the United States (US), while ensuring a strong set of data protection requirements and safeguards. On the basis of this framework EU (and later European Economic Area, EEA) businesses were able to legally transfer personal data to US-based companies that were listed in the Privacy Shield list.

Furthermore, in its judgement the Court provided stricter requirements for the transfer of personal data based on standard contract clauses (SCCs). Data controllers or processors that intend to transfer data based on SCCs must ensure that the data subject is granted a level of protection essentially equivalent to that guaranteed by the General Data Protection Regulation (GDPR) and the EU Charter of Fundamental Rights (CFR) – if necessary with additional measures to compensate for lacunae in protection of third country legal systems. Failing that, operators must suspend the transfer of personal data outside the EU.[5]

Personal data breaches

Personal data breaches by EU companies are of various nature and may occur in the scope of provision of different economic activities. Improper processing of biometric data in a sports club, improper ways of consent obtaining for advertisement provision, conclusion of data processing agreements with laboratories located out of state are the examples of possible data protection breaches.

Here are some cases of data breaches across EU. The State Data Protection Inspectorate (SDPI) of Lithuania has carried out an investigation into processing of biometric personal data in a sports club and imposed a fine in the amount of EUR 20,000 on the sports club for the identified violations of the General Data Protection Regulation (GDPR). The fine was imposed for

---

[4] See full text at: https://curia.europa.eu/juris/documents.jsf?oqp=&for=&mat=or&lgrec=en&jge=&td=%3BALL&jur=C%2CT%2CF&num=C311%252F18&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=en&avg=&cid=4402299

[5] https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

infringements of the provisions GDPR articles related to processing of biometric data without voluntary consent of the data subjects and a failure to ensure other requirements for the valid consent, improper implementation of the data subjects' right to be informed of data processing. It has also been determined that the company has not carried out an assessment of the impact of data processing on data protection, has failed to maintain records of activities.

SDPI received a notification from a natural person stating that in order to use the services of the sports club belonging to the company, fingerprint scanning is mandatory and there are no other alternative ways of identification in the sports club. SDPI carried out an inspection in relation to a possible infringement of the GDPR. According to the GDPR, biometric data is classified as a special category of data the processing of which, as a general rule, is prohibited except for the terms and conditions provided for in Article 9(2) of the GDPR. The company processed the customers' fingerprint models on the basis of the data subject's consent, i.e. on the grounds set forth in Article 9(2)(a) of the GDPR. The SDPI has noted that if the data controller relies on the data subject's consent as a condition of lawful data processing, it should ensure that the data subject's consent met the set conditions (voluntary specific, reasonable, informed, unambiguous, provable and withdrawable consent). Having carried out an investigation, the SDPI has determined that the consent to processing of fingerprint models given by the customers is not voluntary and does not satisfy other requirements for the valid consent; therefore, the SDPI has decided that the company unlawfully processes the binary codes of the customers' fingerprints.[6]

The Norwegian Data Protection Authority's inspection of an Oslo hospital revealed that the hospital cannot document satisfactory control of patient data when the hospital needs laboratory services from other countries.

When the hospital or other Norwegian laboratories do not have the necessary expertise to perform analyses required to provide patients with the medical help they need, they use laboratories in other countries. The hospital therefore sends out blood samples or other biological material and patient data for analysis at laboratories located in other countries, both within and outside the EEA. This affects approx. 8,000 patients a year. Nevertheless, this need for outside assistance does not exempt the hospital from its responsibility of ensuring safe and appropriate processing of biological samples and patient data. The Data Protection Authority concluded that the hospital has failed to establish appropriate agreements to ensure correct handling of the hospital's duties and protection of the patients' rights, among other things because the hospital has failed to conclude data processing agreements with laboratories.

In its response to the Data Protection Authority's preliminary inspection report, the hospital agreed to conclude agreements with foreign labs to ensure that all patient data and the patients' biological material are processed in accordance with relevant legislation.[7]

In another case the Norwegian Data Protection Authority has ordered a Norwegian company to improve its solution for obtaining consent in order to comply with the requirements of the GDPR. This was in response to a complaint from an individual, who found she was targeted with advertising from the mentioned company on Facebook and via e-mail. The complainant, who had previously attended a free webinar provided by the company, found she was getting ads on Facebook and via e-mail without having consented to this. This happened despite the complainant repeatedly having asked to have her personal data erased. The Norwegian company claimed that

---

[6] https://edpb.europa.eu/news/national-news/2021/lithuanian-dpa-fine-imposed-sports-club-infringements-gdpr-processing_en

[7] https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-oslo-university-hospital-ordered-amend-agreements_en

anyone who used their services automatically consented to Facebook and e-mail marketing. According to the company, the complainant had therefore already consented to the marketing when she took a course, as this was specified in their privacy policy.

The company advertises via e-mail and Facebook via so-called "targeted audiences". By uploading customer lists to Facebook, the social platform is able to match these lists with existing Facebook profiles and target these profiles with ads. After reviewing the matter, the Data Protection Authority has concluded that this type of obtaining consent is in violation of the GDPR. The regulation requires consent to be freely given and specific.

It is a basic requirement of the GDPR that consent for processing of personal data must be freely given and specific. Data subjects should be able to choose whether they want to consent to marketing when they buy a service. For example, they should be able to consent to one type of marketing via e-mail, without also having to consent to marketing via Facebook.

On this basis, the Data Protection Authority has ordered the Norwegian company to change the way they obtain consent, in order to establish compliance with the requirements of the GDPR. The company has also been ordered to erase all personal data about the complainant.[8]

Key takeaways

The adoption of the EU GDPR has highly contributed to a new culture of data protection and processing and has fundamentally transformed how businesses treat personal data.

The territorial scope of GDPR is broader than within the EU, as it may apply to companies in third countries if these countries or companies operating in them comply with GDPR.

Personal data may be processed only under "lawful basis" which means that EU customers will have more confidence that their personal data is protected and they will be more willing to share their data.

As a conclusion we can state that customers and businesses in European Union benefit from European data protection new regulation, particularly GDPR, as it sets data protection high standards and principles, introduces new tools for data protection safeguards, such as data protection impact assessment, data protection officers, improves cybersecurity standards, regulates and restricts non-secure international data transfers.

[8] https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-order-improve-solutions-consent_en