Data protection

Ioannidis, Nikolaos

Published in:
Border Control and New Technologies. Addressing Integrated Impact Assessment

DOI:
10.46944/9789461171375.4

Publication date:
2021

4 Personal data protection

Nikolaos Ioannidis
Vrije Universiteit Brussel. E-mail: nikolaos.ioannidis@vub.be.

4.1 Introduction

4.1.1 Definition and development of the right to personal data protection

The terms 'privacy' and 'data protection' are oftentimes understood as one and the same concept. Indeed, the right to personal data protection has evolved from the right to respect for private life, since the development of computers and the Internet in the second half of the 20th century brought considerable risks and new challenges to the latter. To address the need for specific rules about the collection and use of personal information, a new concept of privacy emerged around the 1970s,[1] known in some jurisdictions as 'informational privacy' (i.e. the privacy of personal information usually related to personal data stored in computer systems) or as the 'right to informational self-determination' (i.e. an individual's right to control the disclosure, retention, and dissemination of their personal information[2]). Throughout the years, these concepts evolved and eventually led to the development of special legal regimes that provide for what is known today as 'personal data protection'.

Despite their common origin and overlapping content, privacy and data protection are distinct fundamental rights.[3] While the right to privacy aims to create a personal sphere in which individuals are able to develop their personalities freely, the right to personal data protection is understood as a precondition to the exercising of other rights. In other words, whereas the right to privacy consists of a general prohibition of interference as a 'passive right', the right to personal data protection is considered to be an 'active right', which motivates a system of checks and balances to protect natural persons' personal data.

For the purposes of integrated impact assessment for border control technologies, to which the present textbook is devoted, this Chapter will focus on the right to data protection, and in particular on how it is protected by the General Data Protection Regulation (GDPR).[4] In operationalising the right to data protection, this Chapter follows the structure below. In the following sub-sections, some further introductory notions pertai-

DOI: 10.46944/9789461171375.4

ning to data protection (its importance for society, relevant regulatory instruments and connections with other fundamental rights) are provided. Next, the Chapter delves into specific concepts of data protection law, following the terminology of the GDPR, to guide the assessors throughout the assessment process. Following this, Section 4.1.2 overviews key concepts and actors, Section 4.1.3 looks at principles of EU data protection law, Section 4.1.4 describes legal requirements, and Section 4.1.5 summarises data subject rights.

4.1.2 The importance of data protection in society

Although the right to data protection originates from the need to control the processing of personal information by public authorities, the banking sector, or health insurance companies, nowadays, the same data are processed by big private corporations, including technological companies. The use of artificial intelligence (AI) and profiling algorithms has allowed the processing of large amounts of personal and non-personal data[5] that people commonly share on digital platforms, such as social media sites, e-commerce sites, or health apps. These data have been characterised as "the new oil", as they are exploitable resources for which companies are able to develop strategies to generate revenue and profits.[6] For instance, browsers and websites collect the personal data of users and perform data-driven price differentiation, i.e. the same product or service is offered at different prices depending on the socio-economic status of a person. Another example is the use of recommendation systems upon social media and e-commerce platforms, in which personal data are processed to decide on what to recommend to the end user.

In this context, data protection rules are crucial to ensuring the security of individuals' data and regulating the collection, usage, transfer and disclosure of personal data. Such rules would permit individuals to maintain some control over their personal information and how this is shared with others, as well as make them aware that certain public authorities and private entities collect their data.

4.1.3 The role of data protection in the benchmark

The need for data protection rules is particularly pressing in the context of border control, where so-called 'smart borders', which store personal data, e.g. names and surnames, date, time and place of entry or exit of third-country nationals, travel documents or biometric data, have become widespread. One recurring argument for introducing smart borders is the need for law enforcement authorities to benefit from the best possible tools in order to quickly identify the perpetrators of terrorist acts and other serious crimes.[7] Furthermore, the adoption of pan-European databases would enable the provision of authorised users with fast, seamless, systematic and controlled access to relevant information systems pertaining to individuals who cross borders.

In the light of these developments, focusing on the right to personal data protection as one of the elements of the benchmark of this integrated impact assessment is helpful in controlling for the possible abuse of power by border control authorities and, more generally, in assessing the risks of certain processing operations to the rights and freedoms of natural persons.[8]

The goal of this Chapter is to guide the assessors in assessing whether a given initiative complies with the requirements of necessity and proportionality, accountability, and data protection principles such as purpose limitation and quality of data.[9] A robust assessment is critical when developing new instruments that rely on the use of information technology; the approach provided in this textbook aims to embed personal data protection rules in the technological basis of a proposed instrument.

4.1.4 List of relevant regulatory instruments and systems

To guide the assessors, this Section provides a brief overview of data protection regulatory instruments and systems. As with the right to privacy, the right to personal data protection is not universally protected by a single piece of legislation, but by a multitude of provisions depending on the jurisdiction. This Section follows a tripartite and hierarchical categorisation, through i) international, ii) regional, and iii) national laws.

International law

United Nations: The UN has not explicitly recognised the right to personal data protection as such, in contrast to the right to privacy.[10] Only recently, in 2013 and after the Edward Snowden revelations,[11] the UN adopted the resolution "The Right to Privacy in the Digital Age", while the General Assembly affirmed that the rights held by people offline must also be protected online. Consequently, it called upon all contracting parties to respect and protect the right to privacy in digital communication.[12] This is the closest semblance to modern data protection laws issued by the UN to date.

Council of Europe: Along with the ECHR,[13] the Council of Europe adopted, in 1981, the "Convention for the protection of individuals with regard to automatic processing of personal data" (Convention 108). This Convention is the first and, to this day, only international legally binding instrument dealing with data protection.[14] The Convention underwent a modernisation process, completed with the adoption of an amending Protocol (Convention 108+).[15] Furthermore, the Council of Europe actively issues recommendations with regard to internet actors' accountability.[16]

European Union law

Primary law: The Treaty on the Functioning of the European Union (TFEU) and the Charter of Fundamental Rights of the European Union ('Charter' or CFR) deal with the right

to personal data protection. Article 16 of the TFEU, under the part of the treaty dedicated to the general principles of law, creates a new legal basis, granting the EU the competence to legislate on data protection matters. Article 8 of the Charter enshrines the right to the protection of personal data as a fundamental right.

Secondary law: The body of law founded upon the principles and objectives of the treaties is known as secondary law; this includes, among other things, regulations and directives. From 1995 until May 2018, the principal European Union (EU) legal instrument on data protection was Directive 95/46/EC, also known as the Data Protection Directive.[17] The Directive was adopted on the model of Convention 108, and acted as an instrument for achieving the objectives set by the internal market agenda.

The Directive was replaced by the GDPR,[18] which consolidates principles and rules on data protection, has an extraterritorial effect (i.e. it applies also outside the EU), and enhances the principle of accountability, thus being viewed as an exemplary document for other jurisdictions around the world.

In parallel, three more instruments currently complement the GDPR in data protection matters. First, Directive 2016/680 or the "law enforcement Directive" applies to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Second, Directive 2002/58/EC,[19] also called the "ePrivacy Directive", applies to personal data and the protection of privacy in electronic communications, with regards to security, data breaches and confidentiality of communications (including metadata). Third, Regulation 2018/1725[20] lays down the data protection obligations of the EU institutions and bodies during the processing of personal data by them, and development of new policies (European Institutions Data Protection Regulation (EUDPR)). The principles and key rules of this Regulation do not substantially differ, on the contrary, they are based on the provisions of the GDPR, with the exception of certain provisions inextricably tied to the nature and specificities of the function of EU institutions.

National laws

The first national data protection legislation was a novelty in one (West) German State (Hesse) in 1970. Since then, an increasing number of countries worldwide have progressively enacted (reformed) data protection legislation, including the Member States of the EU. As an illustration, the decade 2010-2019 saw 62 new countries enacting data protection laws, more than in any previous decade. In total, as of today, an impressive number of 142 countries have legislated for data protection.[21] The adoption of firm data protection legislation in parts of the world with significant economic activity is highly important for, among other things, data transfers of personal data, ensuring a consistently high level of protection.

4.1.5 Connection with other fundamental rights

Data protection law does not have the single purpose of protecting only one fundamental right, but rather acts as an umbrella mechanism for multiple fundamental rights whenever affected by the processing of personal data. The interrelationship between the right to personal data protection and other fundamental rights is twofold: (a) since data protection is not an absolute right, it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality, and (b) the EU data protection framework underlines the respect for all fundamental rights; the freedoms and principles recognised in the Charter and as enshrined in the Treaties of the EU. Furthermore, it is assumed that certain types of processing may create significant risks to other fundamental rights and freedoms, therefore explicitly extending the material scope of its protection outside the domain of personal data alone, and towards other fundamental rights and freedoms, when personal data are involved.

Typically, such rights could be: (a) the right to non-discrimination, (b) the freedom of thought, conscience, and religion, (c) the freedom of expression and information, (d) the right to an effective remedy and to a fair trial and (e) the respect for private and family life, home, and communications (right to privacy). Furthermore, it is observed that case law of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR) often involves two or more affected rights. For instance, it is highly probable that a specific type of personal data processing operation does not present risks for a single person but may produce significant societal and legal effects or exacerbate systemic group discrimination. In the realm of border control, the use of automated technologies in identifying migration flows and managing resources is increasingly reinforcing structures of discrimination already inherent in migration decision-making.[22]

4.2 Key concepts and actors

4.2.1 Personal data and data subject

The concepts of personal data and data subject are inextricably linked. 'Personal data' is defined as "information relating to an identified or identifiable natural person".[23] The definition of personal data is extremely broad and may also comprise 'special categories of data'[24] (also called 'sensitive data'), which, by their very nature, may pose greater risks to the data subjects when processed. Due to their character, processing of these data requires higher attention to be afforded by the data controller and other involved parties. These categories of data include personal data 'revealing racial or ethnic origin, political opinions,

religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.[25]

If the processing of data does not concern an identified or identifiable person (a human being), then data protection law does not apply.[26] For example, if the process of anonymisation has been conducted, meaning that all identifying elements are eliminated from a set of personal data, and the data subject is no longer identifiable, then data protection law does not apply. In order to determine whether a natural person is identifiable, one must take into account all reasonable means (including available technology) that are likely to be used to directly or indirectly identify the individual. Establishing a link with a natural person can be achieved by reference to an 'identifier' such as a name, an identification number, locational data, an online identifier or to one or more properties specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.[27]

4.2.2 Data controller

In the context of personal data processing, the key decision-making figure is the data controller. In the private sector sphere, this is usually a natural or legal person, while in the public sector, this is an authority (e.g. a ministry, a governmental agency, etc.). The data controller is the one who determines the means and purposes of processing the personal data of natural persons.[28] This mostly answers the question of 'why' and 'how' the personal data should be processed.[29] To determine whether or not an entity acts as a data controller, the assessors look at the decision to collect or process the personal data, the purpose or outcome of the processing, which personal data is collected and from which individuals, whether there will be a contract for this, which decisions or inferences are drawn during or after processing, etc.

4.2.3 Data processor

A 'data processor' means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the data controller.[30] As a general rule, the data processor processes personal data by only following specific instructions regarding the processing. For instance, data processors do not decide to collect personal data from individuals on their own initiative, do not decide what personal data should be collected from individuals, do not decide the lawful basis for the use of that data, do not decide what purpose or purposes the data will be used for, and do not decide whether to disclose the data, or to whom.[31]

4.2.4 Data protection authorities

EU data protection law is applied and enforced in each national jurisdiction independently. This is ensured by the function of independent supervisory authorities (SAs), also called data protection authorities (DPAs). Specifically, each Member State shall provide for the institution and function of one or more independent public authorities to be responsible for monitoring the proper application and enforcement of data protection laws in their jurisdiction.[32]

Supervisory authorities are tasked with the following activities:[33]

- they promote data protection at the national level, advising data subjects, data controllers and the government;
- they hear complaints and assist data subjects with alleged violations of data protection rights;
- they supervise controllers and processors, and they conduct investigations on the application of the Regulation;
- they monitor relevant (technological) developments, insofar as they impact the protection of personal data, such as the development of information and communication technologies;
- they possess investigative, corrective, authorisation and advisory powers, for example, they may carry out investigations in the form of data protection audits;
- they notify the controller or the processor of an alleged infringement of the Regulation, or obtain, from the controller and the processor access to all personal data and premises (such as data processing equipment and means);
- they can issue warnings to a controller whose intended processing operations are likely to infringe provisions of the Regulation;
- they can impose a temporary or definitive limitation including a ban on processing and,
- they are the ones to impose the administrative fines, where necessary.[34]

4.3 Principles of EU data protection law

4.3.1 Lawfulness, fairness, transparency

Three fundamental principles in data protection law jointly act as the starting point for the more detailed provisions on processing. Largely, these concern the data controller. The most important are i) lawfulness, ii) fairness and iii) transparency. Their general articulation as principles is further specified according to the circumstances in which they are applied. In other words, their application in the area of border control entails different risks compared to personal data processing for marketing purposes.

In order to process personal data, the data controller must have a lawful basis to do so. This basis functions as an enabler for processing personal data within the scope of the purposes identified. Lawful processing requires the consent of the data subject or one of the five other legitimate grounds provided in the data protection legislation. It also implies that the data controller has reviewed the purposes of the processing activities, and has selected the most appropriate lawful basis (or bases) for each activity.

Personal data must be processed fairly. This means that processing must be done in ways that people would reasonably expect, and not in ways that have unjustified adverse effects on them, or in ways that could mislead them. This does not mean, however, that every processing that would negatively affect an individual should be considered 'unfair'.

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used.[35] Among other things, the following information is provided beforehand: the identity and the contact details of the controller, the purposes of the processing for which the personal data are intended, and also the legal basis for the processing, the legitimate interests pursued, the legitimate interests, the period for which the personal data will be stored, etc.[36] Transparency in processing facilitates the exercising of the data subject's rights.

4.3.2 Purpose limitation

The principle of purpose limitation means that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In other words, any processing of personal data must be performed for a specific well-defined purpose, and if this happens for additional purposes, these must be specified and compatible with the original one.[37] Its objective is primarily legal certainty, along with predictability and user control.[38] Neither processing personal data for undefined or unlimited purposes is lawful, nor is processing based on the assumption that it may be useful at some point in the future.

It is the data controller who defines the purposes of processing. In assessing the compatibility of the initial specific purpose with any additional ones, the controller shall take the following into consideration: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected; the reasonable expectations of data subjects; the nature of the personal data; the consequences of the processing for data subjects; the existence of appropriate safeguards.[39]

4.3.3 Data minimisation

Data minimisation means that personal data shall be adequate, relevant and limited to what is *necessary* in relation to the purposes for which they are processed. All these three words, '*adequate, relevant and limited*' are subject to the discretionary power of by the data controller. The criteria for the assessment of necessity of processing are not straightforward, and neither is the extent to which the purpose of the processing can be reasonably fulfilled by other means. What is deemed 'appropriate' in the case of extensive processing systems is not listed, in order to avoid prescriptiveness and to allow greater conformity with technological advancements. The data controller shall proceed to an assessment of the measures adopted, so as to ensure that data processing does not entail a disproportionate interference in the fundamental rights and freedoms at stake. This also includes periodic review of the stored data, and deletion of those that are not necessary.

4.3.4 Data accuracy

A data controller must ascertain that data are accurate and kept up-to-date by guaranteeing that data that are inaccurate are erased or rectified without delay.[40] At the same time, some categories of personal data shall remain non-updated (e.g. a medical record that should be compared to and complemented by future examinations). The data subject shall have the right to restriction of processing by the controller when the accuracy of the personal data is contested.[41]

4.3.5 Storage limitation

The data controller shall ensure that personal data are deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected. Personal data shall be kept in a form that permits identification of data subjects for no longer than what is necessary for the purposes for which the personal data are processed. Storage limitation functions in conjunction with purpose limitation, since these both allow for the same exception of further processing solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.[42] Data subjects must be appropriately informed about the standard retention periods through the privacy policy.[43] This principle enables compliance with individuals' requests for erasure under 'the right to be forgotten'.

4.4 Legal requirements

4.4.1 Lawfulness of processing

Pursuant to the principle of lawfulness, personal data may be lawfully processed if they meet one of the following criteria (lawful grounds):[44]

a) *Consent*: the data subject has given consent to the processing of their personal data for one or more specific purposes. Consent is considered freely given if the data subject has genuine or free choice or is able to refuse or withdraw consent without detriment.[45] It shall be as easy to withdraw as to give consent, at any time. Consent may not always be a lawful ground: for instance, employees are not in a position to freely give, refuse or revoke consent, given their dependency within the employer/employee relationship. Consent must also be informed (data subjects must have received sufficient information), specific (for concrete processing purposes) and unambiguous (without reasonable doubts).

b) *Contract*: processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract. This lawful ground applies where either of two conditions are met: the processing in question is objectively necessary for the performance of a contract with a data subject, or the processing is objectively necessary in order to take pre-contractual steps at the request of a data subject.[46]

c) *Legal obligation*: processing is necessary for compliance with a legal obligation to which the controller is subject. For instance, employers must process data about their employees for social security and taxation reasons, and businesses must process data about their customers for taxation purposes.[47]

d) *Vital interests*: processing is necessary in order to protect the vital interests of the data subject or of another natural person. An illustration would be when monitoring epidemics and their development, or where there is a humanitarian emergency.[48]

e) *Public interest*: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is most relevant to public authorities, and the underlying task, function or power must have a clear basis in law. Furthermore, there should be no less intrusive way by which an authority is able to reasonably perform its tasks or exercise its powers.

f) *Legitimate interest*: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child. In this respect, the legitimate interests of the controller are first identified, and then a balancing exercise must be conducted between those interests and the interests or fundamental rights and freedoms of the data subject. A classic example of legitimate interest is direct marketing.

4.4.2 Accountability and compliance

The principle of accountability[49] stipulates that the data controller shall be responsible for, and be able to demonstrate compliance with, all the data protection principles mentioned above. This means that they shall actively and continuously implement measures to promote and safeguard data protection in their processing activities. Demonstrating compliance with the Regulation is an obligation towards data subjects, but also towards the data protection authorities. Three prominent newly introduced tools for accountability include the data protection officer, the data protection impact assessment, and the data protection by design & by default.

Security of processing

The principle of data security is probably the most complicated and disputed one. It is connected to a data protection principle, that of integrity and confidentiality. It requires that the security, integrity and confidentiality of personal data is guaranteed, so as to prevent adverse effects for the data subject. Measures adopted could be either of a technical or an organisational nature. The appropriateness of security measures must be determined on a case-by-case basis and be reviewed regularly.

Criteria for such choice are the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Measures that are deemed technically appropriate, among others, are: the pseudonymisation and encryption, the confidentiality, integrity, availability and resilience of processing systems and services, restoration of the availability and access to personal data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[50]

Measures that correspond to good organisational rules could be: regular provision of information to all employees about data security rules and their obligations under data protection law, especially regarding their confidentiality obligations, clear distribution of responsibilities and a transparent outline of competences in matters of data processing, and ensuring that authorisations to access personal data have been assigned by the competent person and require proper documentation.[51]

Data protection officer

The role of the data protection officer (DPO) has been formulated in such a way so as to be the key role in the accountability mechanism. DPOs are responsible for the due completion, and liable for reporting the success of a compliance project, yet without being accountable themselves. It is the data controller who is accountable for the compliance of the processing operations with the law. DPOs are obligatorily appointed where processing is conducted by a public authority, where processing results in systematic monitoring, or

where the processing concerns special categories of data or personal data relating to criminal convictions or offences.[52]

DPOs are independent: they do not receive instructions from the management, they facilitate compliance by implementing the rules and communicating with the supervisory authorities, while they are involved, properly and in a timely manner, in all issues which relate to the protection of personal data within the organisation.[53] Duties of DPOs include, for example, advising on the undertaking of data protection impact assessments, training personnel, and creating and maintaining records of processing activities within an organisation.

Data protection impact assessment

The requirement to conduct data protection impact assessments (DPIAs) in several innovative laws around the world is not coincidental. The recently reformed personal data protection law in the EU introduced a requirement for data controllers to assess the impacts of data processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons" with regard to the protection of personal data.[54] The level of risk varies depending on the nature and scope of processing. Large-scale operations and those involving the processing of sensitive data present much higher risks for data subjects compared to smaller-scale data controllers who processes their employees' personal phone numbers.

The Regulation foresees a list of processing operations that are considered high-risk and for which a prior impact assessment is necessary: where there is systematic and extensive evaluation of personal aspects (profiling), where special categories of data or personal data relating to criminal convictions or offences are processed, and where processing involves the large-scale, systematic monitoring of publicly accessible areas.[55] The content of the impact assessment shall include, among other things, an assessment of the necessity and proportionality of the processing operations and the possible risks to the rights of individuals, as well as mitigation measures for the risks identified. To demonstrate compliance, data controllers must maintain a record of the processing activities carried out under their responsibility.[56]

Data protection by design and by default

Data protection by design and by default refers to the effective implementation of data protection principles and appropriate technical and organisational measures to safeguard data subjects' rights and freedoms. The concept is an evolution of what was previously known as privacy by design, and is currently a legal requirement. It is inspired by the fair information practices, as articulated by the Information and Privacy Commissioner of Canada.[57]

Data protection 'by design' applies to the development of new services, systems, processes or products that involve personal data processing. It involves implementation of appropriate technical and organisational measures designed to implement the data protection principles, and the integration of safeguards into the processing necessary to fulfil

the legal requirements and protect data subjects' rights. This way, privacy and data protection are guaranteed at the design phase of any system, service, product or process, and then throughout the lifecycle.

Data protection 'by default' requires that the data controller ensures processing of the data that is necessary to achieve a specific purpose. It links to the fundamental data protection principles of data minimisation and purpose limitation. A misunderstanding could be that it requires the adoption of a 'default to off' solution, but this is not true: This principle translates as the need to specify the personal data before the processing starts, to appropriately inform individuals, and to only process the data that are needed for the purpose.[58]

Data breaches

One additional accountability mechanism is that relating to data breaches. A personal data breach refers to a security breach leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure or access to processed personal data.[59] Data breaches can be highly detrimental to the data protection rights of individuals who, as a result of the breach, lose control over their personal data. They are subsequently exposed to risks, such as identity theft or fraud, financial loss or material damages, loss of confidentiality of personal data protected by professional secrecy, and damage to their reputation.[60]

When a personal data breach is detected, and if it 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. The notification must include a description of the nature of the data breach, of data subjects affected, and a description of the possible consequences. If the data breach is likely to result in high risks for the data subjects, then the data controller must inform the data subjects in clear and plain language. At the same time, the controller is responsible for informing the supervisory authorities.

4.4.3 Data transfers

The level of protection of personal data is deemed to accompany them in function of the country that the personal data are. Data protection law regulates transfers of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation.[61] In other words, if and whenever personal data are transferred outside the EU, then they are subject to specific rules in processing. With regard to the principle of free movement of personal data in the EU, this shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.[62]

Depending on the recipient of personal data, there are different tools to frame the data transfers. The strongest, but also the least common, is the adequacy decision.[63] A third country may be declared as offering an adequate level of protection, under a European

Commission decision, meaning that data can be transferred to another company in that third country without the data exporter being required to provide further safeguards or conditions.[64] If an adequacy decision has not been signed, then data controllers can transfer personal data based on binding corporate rules,[65] which are legally binding to every member of the group. Alternatively, they can use standard contractual clauses approved by the European Commission; lastly, it is possible to adhere to a code of conduct or certification mechanism.

Data transfers are subject to the discretion of the data controller ("…has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available"). This means that the burden of proving that, by transferring personal data to third countries, the level of protection there fulfils the minimum requirements in the EU – first and foremost, that data subject rights are not prejudiced and that appropriate remedies are in place – lies upon the data controller. In such cases, a data transfer impact assessment, a risk assessment of the factors related to the transferral of data to third countries, may be needed to complement the DPIA or as a standalone document. In this, the necessity, proportionality, and technical and organisational measures are evaluated, as well as the level of protection of fundamental rights.

4.5 Data subject rights

4.5.1 Right to be informed

The transparency principle requires that any personal data processing should generally be transparent to individuals. To this end, the data controller is obligated to provide information to the data subjects. This holds whether personal data are collected from the data subject directly or have not been obtained from the data subject, but instead from third parties. Such an obligation does not depend on a request from the data subject.[66] Rather, the controller must proactively comply with the obligation, regardless of whether the data subject shows an interest in the information or not.

A broad comprehensive obligation is established when communicating this information to data subjects.[67] As described in the transparency principle, data controllers must provide, at the time the data are obtained or prior to the processing, in concise, transparent, intelligible, easily accessible, clear, plain and easily understandable language, all the necessary information, usually in the form of a privacy notice or a website privacy policy. This information is provided free of charge. Frequently, information on data processing is structured in such a way so as to respond to the following questions: *Who are we? What data do we collect from you? Why are we collecting your data? How do we process your data? What are your rights?*

4.5.2 Right of access by the data subject

The right to access one's own data (right of access) is a pivotal right[68] and is also set out as one of the elements of the fundamental right to the protection of personal data in the Charter of Fundamental Rights, i.e. in primary law.[69] The right of access gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps data subjects to understand how and why the data controller is using their data, and check whether this is being done lawfully. The data controller must provide, upon request by the data subject, at least information on the following: purposes of processing, categories of personal data processed, recipients of the data, storage periods, existence of data subject rights, and the logic involved in automated processing of data, in the case of automated decisions.[70]

4.5.3 Right to rectification

EU law provides for a right to rectification of personal data.[71] The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning them. This right includes completing data which were previously incomplete, or inaccurate personal data, which must be rectified without undue or excessive delay.

4.5.4 Right to erasure ('right to be forgotten')

Data subjects have the right to have their own personal data erased, pursuant to the principle of data minimisation.[72] This is applicable, for instance where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, the data subject withdraws consent, or the data has been unlawfully processed.[73] Nevertheless, this right is not absolute: it needs to be balanced against other bases, such as the freedom of expression, the public interest, scientific or historical research purposes or statistical purposes.

4.5.5 Right to restriction of processing

Data subjects are entitled to obtain from the controller restriction of processing of their personal data where the accuracy of the personal data processed by the data controller is disputed or is unknown, the processing itself is unlawful, the processing of personal data is not necessary for the purposes intended, or the data subject has objected to the processing.[74] This right enables the data subject to limit the way that a data controller uses their personal data, often as an alternative to deleting them.

4.5.6 Right to data portability

Applying the right to data portability essentially means that data subjects are entitled to have their personal data transmitted directly from one controller to another if this is technically feasible. This involves receiving the personal data in a structured, commonly used and machine-readable format and then transmitting those data to another controller without hindrance. The right to data portability is permitted when the lawful basis is either consent or contract, and the processing is carried out by automated means.[75]

4.5.7 Right to object

Data subjects have the right to object to the processing of their personal data in certain circumstances, such as where a task is carried out in the public interest, or in the exercising of official authority or legitimate interests. The right to object is raised to an absolute right in the case of direct marketing.[76] The right to object serves in striking the correct balance between the data subject's data protection rights and the legitimate rights of the data controller. Furthermore, it constitutes a powerful weapon against profiling.

4.5.8 Right not to be subject to automated decision-making, including profiling

In principle, data subjects must not be subject to automated decisions that give rise to legal or similarly significant effects.[77] This right is passive, in the sense that it equates to a general prohibition and does not require the data subject to proactively seek an objection to such a decision.[78]

This provision could concern, for instance, an automatic refusal of an online credit application or e-recruiting practices. Automated decision-making based on profiling may take the form of analysing or predicting aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, etc. If such processing is conducted, it must be accompanied by adequate safeguards for the data subject, such as the right to obtain human intervention on the part of the controller, to express their point of view, and to contest the decision.[79]

4.5.9 Data subject rights in border control

The national DPAs supervise the application of the data protection rules in their respective countries, while the EDPS monitors the application of the data protection rules for the central system managed by eu-LISA.[80] In accordance with data protection principles, all

individuals whose data is processed in the Schengen Information System II are accorded specific rights. These rights are: a) the right of access to data relating to them stored in SIS II; b) the right to correction of inaccurate data or deletion when data have been unlawfully stored; c) the right to bring proceedings before the courts or competent authorities to correct or delete data, or to obtain compensation.

Lastly, data subject rights do not always prevail, they are not absolute; restrictions may be imposed, particularly when other interests are at stake. Such restrictions shall respect the essence of the right to data protection (its core) and shall be necessary and proportionate measures in a democratic society. Common grounds for imposing restrictions on data subject rights are national and public security, prevention, investigation, detection or prosecution of criminal offences, defence, protection of judicial independence, and protection of the data subject or the rights and freedoms of others.

Endnotes

1. The first data protection legislation in the world was passed in 1970, in the (West) German state of Hesse.
2. Alan F. Westin, "Privacy and Freedom", *Washington and Lee Law Review* 25, no. 1 (1967): 166-170, https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?Article=3659&context=wlulr.
3. European Union Agency For Fundamental Rights, European Court of Human Rights, and European Data Protection Supervisor, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018), https://doi.org/10.2811/58814.
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, and repealing Directive 95/46/EC. OJ L 119, 4.5.2016, p. 1–88.
5. Maja Brkan, "Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond", *International Journal of Law and Information Technology* 27, no. 2 (2019): 91–121, https://doi.org/10.1093/ijlit/eay017.
6. Jathan Sadowski, "When Data Is Capital: Datafication, Accumulation, and Extraction," *Big Data and Society* 6, no. 1 (2019): 1–12, https://doi.org/10.1177/2053951718820549.
7. European Data Protection Supervisor (EDPS) *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems* (2018), https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf.
8. *European Commission Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security* (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0205&from=EN.
9. Ibid.
10. The main instruments of the United Nations (UN), stipulating provisions about privacy, are the non-binding Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

11. These revelations have increased public concern about information security and privacy resulting from disclosures detailing the extent of the National Security Agency's (NSA) surveillance activities.
12. United Nations (UN), The Right to Privacy in the Digital Age, http://undocs.org/A/RES/68/167.
13. The right to personal data protection is not enshrined in the European Convention on Human Rights (ECHR) *per se*. Rather, it is inferred from the scope of Article 8, which guarantees the right to respect for private and family life, home and correspondence.
14. Ibid.
15. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).
16. The precautionary measure of human rights impact assessment is stipulated in 'Recommendation CM/Rec (2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.'
17. 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, OJ L 281, 23.11.1995, p. 31–50.
18. 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.
19. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
20. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
21. Graham Greenleaf, "2020 Ends a Decade of 62 New Data Privacy Laws," *Privacy Laws & Business International Report* 163 (2020): 24-26, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611.
22. Petra Molnar, *Technological Testing Grounds, Migration Management Experiments and Reflections from the Ground Up* (2020), https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf.
23. GDPR, Art. 4 (1).
24. GDPR, Art. 9.
25. GDPR, Art. 9 (1).
26. Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", WP 136, 20 June 2007, p. 22.
27. GDPR, Art. 4 (1).
28. GDPR, Art. 4 (7).
29. Information Commissioner's Office (ICO), Controllers and processors, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/.
30. GDPR, Art. 4 (8).
31. Information Commissioner's Office (ICO), Controllers and processors, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/.
32. GDPR, Art. 51.
33. GDPR, Art. 57-58.
34. GDPR, Art 83.

35. GDPR, Art. 12 (1).
36. GDPR, Art. 12 (2) and Recital 58.
37. GDPR, Art. 5 (1) (b).
38. Ibid.
39. GDPR, Recital 50.
40. GDPR, Art. 5 (1) (d).
41. GDPR, Art. 18 (1) (a).
42. GDPR, Art. 5 (1) (e).
43. Information Commissioner's Office (ICO), Controllers and processors, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/.
44. GDPR, Art. 6 (1).
45. GDPR, Recital 42.
46. 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, adopted on 9 April 2019, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf.
47. Ibid.
48. Ibid.
49. GDPR, Art. 5 (2).
50. GDPR, Art. 32 (1).
51. Ibid.
52. GDPR, Art. 37 (1).
53. GDPR, Art. 37 (3) and (4).
54. Dariusz Kloza et al., "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals."
55. GDPR, Art. 35 (1).
56. GDPR, Art. 30.
57. Ann Cavoukian, "Privacy by Design, the 7 foundational principles implementation and mapping of fair information practices", https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf.
58. Information Commissioner's Office, "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/#dpd3.
59. GDPR, Art. 4 (12).
60. GDPR, Recital 75.
61. GDPR, Art. 44.
62. GDPR, Art. 1 (3).
63. GDPR, Art. 45.
64. The European Commission has so far only recognised Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay as providing adequate protection.
65. Information Commissioner's Office, Binding Corporate rules, https://ico.org.uk/for-organisations/binding-corporate-rules/#:~:text=Binding%20Corporate%20Rules%20(BCRs)%20are,Directive%2095%2F46%2FEC.
66. European Union Agency for Fundamental Rights, Council of Europe-European Court of Human Rights, European Data Protection Supervisor, "Handbook on European Data Protection Law", 207.
67. GDPR, Art. 12-14.
68. GDPR, Art. 15.

69. Charter of Fundamental Rights, Art. 8 (2).
70. GDPR, Art. 15.
71. GDPR, Art. 16.
72. European Union Agency for Fundamental Rights – Council of Europe-European Court of Human Rights – European Data Protection Supervisor.
73. GDPR, Art. 17.
74. GDPR, Art. 18.
75. GDPR, Art. 20.
76. GDPR, Art. 21.
77. GDPR, Art. 22.
78. Article 29 Working Party, "Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679", WP 251, 3 October 2017, p. 15.
79. General Data Protection Regulation, Art. 22 (3).
80. European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA).