SELF-EXCLUSION MECHANISM and GDPR PRINCIPLES

Dusan Pavlovic
Self-Exclusion Mechanisms and GDPR Principles

Author: Dusan Pavlovic

Creation of this white paper was fully supported by International Center for Gaming Regulation, University of Nevada, Las Vegas

July 2019
Contents

Part One – Introduction .................................................................................................................. 3
  1. Introduction to the research .................................................................................................. 3
  2. Research question and impact ............................................................................................ 5
  3. Methodology and outline of the study .................................................................................. 7

Part Two – The GDPR and Its Principles .................................................................................... 9
  1. The GDPR – What, when, where, how and why ................................................................. 9
  2. The GDPR – Key terms ....................................................................................................... 12
  3. GDPR principles in detail .................................................................................................... 15
    3.1 Lawfulness, fairness and transparency ........................................................................... 15
    3.2 The purpose limitation principle .................................................................................... 24
    3.3 Data minimization ........................................................................................................... 27
    3.4 Data accuracy .................................................................................................................. 28
    3.5 The storage limitation principle ....................................................................................... 30
    3.6 Confidentiality and integrity ........................................................................................... 31

Part Three – A Typology of Self-Exclusion Mechanisms .......................................................... 36
  1. What is a self-exclusion mechanism? .................................................................................. 36
  2. Identification and regulation as cornerstones of self-exclusion ......................................... 37
    2.1 Horizontally disconnected; vertically unregulated ......................................................... 39
    2.2 Horizontally connected; vertically unregulated ............................................................... 41
    2.3 Horizontally connected; vertically regulated ................................................................. 43
    2.4 Horizontally disconnected; vertically regulated ............................................................. 46

Part Four – When the GDPR Meets Self-Exclusion Mechanisms ........................................... 50
  1. Lawfulness, transparency and fairness ............................................................................... 50
  2. The purpose limitation principle ....................................................................................... 54
  3. Data standards .................................................................................................................... 56
  4. Security and confidentiality ................................................................................................. 58
  5. Accountability .................................................................................................................... 63

Part Five – Conclusion ................................................................................................................. 65

Bibliography ............................................................................................................................... 68
Part One – Introduction

1. Introduction to the research

The last decade has witnessed a tectonic shift in European Union data protection regulation. The pace of development of emerging technologies and the effects of their implementation have affected social, economic, legal and political areas. Therefore, regulating new technologies is more relevant now than ever before. Regulators must deal with the challenge of creating balance between responsible innovation and the use of technologies for lucrative purposes. In many respects, conventional legislative techniques have been disrupted, and hence many stakeholders are looking for alternatives in self-regulation. In addition, the cross-border movement of goods and services generates a need for the harmonization (and in some cases the unification) of national legislative frameworks. Advocacy with regard to international and supranational sources of technology regulation thus appears to be a reasonable solution.

The European Union is one of the most influential organizations in Europe. A fundamental feature of this organization is EU law – a system of laws operating within the 28 Member States of the European Union. In general, this system overrules national legislative frameworks in cases of conflict. For this reason, national legislative systems have been harmonized, and in certain matters unified. As a response to the rapid development of emerging technologies, in recent years EU legislators have reformed EU data protection regulations in order to empower European citizens to exercise their rights regarding the processing of their personal data. The highlight of these reforms was the adoption of the General Data Protection Regulation (GDPR).\(^1\) Apart from empowering European citizens concerning their data protection rights, the GDPR provides a singular system of personal data protection for all 28 Member States.

Whereas the system of EU data protection regulation has been progressing towards the harmonization and unification of national legislative frameworks, the situation is different when it comes to EU gambling regulation. Indeed, many would argue that EU gambling law does not exist and that regulative initiatives to harmonize EU Member State national gambling legislations have failed. Member States have been striving to regulate gambling activities on their own, at the national level. They have called upon different social, cultural, and political features of gambling to justify using the principle of subsidiarity to regulate

gambling at the national level. By doing so, they have avoided harmonizing national legislative frameworks in the domain of gambling, including online gambling. The relation between EU initiatives to harmonize gambling regulations and Member States’ regulative aspirations has been described as a “tug of war without a winner.” As a result, online gambling (as a service with various distinctive attributes) is controlled, organized and regulated exclusively at the national level. The current state of gambling regulation can be described as legislatively fragmented (28 Member States with 28 gambling legislative frameworks), as being in tension with the principle of freedom to provide services in the EU. This approach is officially justified by the need to protect national policies (e.g. public health policies, youth policies, etc.). Alongside the principle of subsidiarity, the cornerstones for regulating gambling at the national level are provided by several rulings made by the European Court of Justice (CJEU). CJEU case law can be viewed as giving carte blanche to Member States, with only some limitations being placed on them regarding the regulation of gambling in accordance with national policies.

The processing of online gamblers’ personal data by online gambling service providers is necessary for the functioning of the service. Anyone who intends to gamble online must register and open a personal account. Online gambling service providers request several different pieces of personal data for registration purposes. The EC Recommendation laid down that following this registration, all player activity must be monitored by a gambling operator. Operators must be able to inform players and alert them of their winnings and losses and the duration of their play. This sort of information must be sent on a regular basis. Whenever gambling behavior indicates the risk of a gambling disorder, players should be supported and offered professional assistance. In addition, players can themselves set up limits to their own gambling activities by using self-exclusion mechanisms.

Processing as much personal data as possible provides a greater opportunity to promote responsible gambling practices. Self-exclusion mechanisms are one of the most important measures in responsible gambling practices.

---

7 Ibid, art 25.
8 Ibid, sec VII.
gambling, and the proper identification of gamblers is necessary for reliably identifying those who have prohibited themselves from gambling for a certain period.

From an EU regulatory perspective, there is a dichotomy between the functioning of self-exclusion mechanisms on the one hand and processing online gamblers’ personal data on the other. Because gambling regulation in the EU is so fragmented, whereas data protection regulation is unified, it is reasonable to raise doubts about the effective functioning of self-exclusion mechanisms in Europe. From a practical perspective, the functioning of self-exclusion mechanisms is regulated by 28 different states and (who knows how many) self-regulation systems. For that reason, there are many difficulties when it comes to reliably identifying self-excluded online gamblers. From the perspective of data protection regulation in the EU, however, a unique system of rules concerning personal data processing should be applicable to all self-excluded online gamblers in the EU. This study aims to reveal the conflicting interests among two regulatory fields, identifying the practical consequences of the current regulatory states. It goes on to suggest practical solutions to potential conflicts between data protection regulation and gambling regulation in terms of the functioning of self-exclusion mechanisms.

2. Research question and impact

This study aims to demonstrate the relation between the implementation of the general principles of the GDPR on the one hand and the effectiveness of self-exclusion mechanisms on the other. The goal is to shed light on how the application of GDPR principles affects different types of self-exclusion mechanisms with regard to their organizational and regulatory aspects. Thus, the study considers the tension between ensuring the effectiveness of self-exclusion mechanisms and protecting the right to privacy with regard to gamblers’ personal data. To this end, the research focuses on the following general question:

- How does the application of GDPR principles affect the effectiveness of self-exclusion mechanisms?

To answer the main research question, the following sub-questions will also be considered:

- What is the GDPR?
- What are the data protection principles set out by the GDPR?
- What is a self-exclusion mechanism, and how can it be organized/regulated?
- What are the features (advantages and disadvantages) of different self-exclusion mechanisms, taking into account their organizational and regulatory aspects?
What hypothesis have been made regarding the effectiveness of self-exclusion mechanisms in the context of the transfer of personal data relating to self-excluded online gamblers and the regulation of self-exclusion mechanisms?

How do each of the GDPR principles affect the functioning/effectiveness of each of the proposed self-exclusion mechanisms?

The significance and impact of this research is very broad. For one, this study is the first of its kind. For the first time, GDPR principles will be discussed in the context of the functioning and effectiveness of self-exclusion mechanisms. The study thus provides an innovative and original contribution to the field.

The second reason lies in the fact that online gambling services are difficult (or even impossible) to regulate when we move beyond the micro (i.e. the national or regional) level. Given the legislative fragmentation of gambling regulation in the EU, grounded in the exclusive regulatory control held by EU Member States, there are few sources of EU law that are applicable to online gambling services. With this said, the purpose of the GDPR was to unify the regulation of personal data protection in the EU. This study thus centers on two separate fields of regulation: a system in which the same (or similar) legal norms are applicable in several countries (personal data protection), and a system that varies from state to state (online gambling services and self-exclusion mechanisms). As a result, the study reveals the challenges that accompany the comprehensive regulation of online gambling through national legislative frameworks. This is due not only to the nature of the industry (the operations of which are not easily constrained within political borders) but also to the regulatory frameworks at the supranational level (such as the EU), which tend to be international legal standards.

This white paper helps to clarify the relationship between personal data processing regulation on the one hand and the regulation/organization of self-exclusion mechanisms on the other. It will help to raise awareness, on the part of stakeholders in the online gambling domain (among others), about personal data regulation and its influence on one of the most common measures of responsible gambling – the implementation of self-exclusion mechanisms. The study will therefore contribute significantly to overcoming legislative obstacles to creating further effective self-exclusion mechanisms and related regulatory frameworks. In this regard, the study identifies opportunities for sharing online data in ways that do not conflict with GDPR principles.

Finally, this study contributes to our understanding of the effective regulation of technology. New technologies are being used to process personal data, including data related to online gamblers and self-
excluded online gamblers. The rapid development of technology continually challenges attempts at effective regulation. It is reasonable to expect that new technologies will improve the processing of online gamblers’ data. Thus, this study identifies data protection requirements that must be met by public and private regulators when shaping new regulatory frameworks for the implementation of emerging technologies (in particular, those used to process the personal data of self-excluded online gamblers).

3. Methodology and outline of the study

The following analysis of the relevant data protection principles, the various self-exclusion mechanisms, and the connections between these principles and mechanisms requires several research methodologies. This study deploys desk research and legal research. Because the analysis is based on sources from the fields of law and information technology, the study has a multidisciplinary character. The author is a lawyer with expertise in the fields of data protection and gambling regulation. He also has considerable practical experience in information technology and has familiarized himself with issues in this field by consulting the relevant literature and experts.

This study contains five parts. Each part is composed of various sections and subsections.

The first part briefly introduces the topic, the study’s methodology, and its central research question. This provides an outline of the study and introduces the reader to the purpose and general importance of the study, along with the means used for its development.

The second part concerns the General Data Protection Regulation and its principles. In this part, descriptive legal research is applied in order to examine this source of EU data protection regulation. The second part begins with a brief historical interpretation of data protection regulation in Europe and around the globe. Following this, attention is given to the contemporary perspective of data protection regulation in Europe. The study presents the main principles of the GDPR insofar as they depict the core values of the regulation and shape the spirit of the law.

The third part of the study is analytical in character. It presents a novel typography of self-exclusion mechanisms based on two dimensions – one vertical (regulatory), the other horizontal (data connectivity). The study presents four distinctive types of self-exclusion mechanisms.

The fourth part is also analytical. It provides the author’s view on how GDPR principles affect different types of self-exclusion mechanisms. This part is crucial to answering the general research question.
Finally, the fifth part of the study summarizes the presented findings and concludes the main points, revealing the study's qualitative nature.

All presented results and claims are unquantified, open to argumentation and suitable for further research.
Part Two – The GDPR and Its Principles

1. The GDPR – What, when, where, how and why

On 25 May 2018, the General Data Protection Regulation, known as the GDPR, became fully effective. At the time, the relevant stakeholders were speaking out (many of them quite spiritedly) about this new source of European Union data protection regulation. The GDPR was a new regulation at the time and introduced certain novelties into EU law, industry, policy, economy and other sectors. This regulation created a new set of rules and redesigns so as to provide greater power to people when it came to processing their data. As a result, companies and states (as stakeholders with the greatest interest in processing personal data) are now required to be at least more transparent when processing personal data.

The GDPR is a source of unification of EU data protection law. This means that national states do not need to transpose general regulatory principles into their national legislation (this is a typical feature of EU directives) in order to implement EU law. Regulations like the GDPR thus have a certain supremacy over national legislation and apply automatically to all 28 Member States of the EU. Taking into account the fact that the GDPR enshrines very high standards for personal data protection, many policy makers and stakeholders have recommended that this source become the international standard for personal data protection.

The GDPR did not emerge out of the blue. If we take a brief survey of the development of data protection legislation and the relevant legal sources on the protection of personal privacy in Europe, the GDPR emerges as a predictable continuation of the endeavor to protect human rights. As a starting point in explaining the origins of the GDPR, we should begin with the Universal Declaration of Human Rights, adopted by the United Nations just few years following the end of World War II. Article 12 of the Declaration lays down that “no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.” This article opened the door for the protection of personal privacy, which has been further developed by other international, supranational and national legal sources. What is important here is that the Declaration enshrines the idea that

---

10 Ibid, art 12.
individual rights and freedoms are not absolute and may be constrained. This is clearly stated in article 29(2).

The European Convention on Human Rights (ECHR) entered into force in September 1953. All Council of Europe states are party to the ECHR. “Respect for private and family right” is included within the scope of rights and freedoms protected by ECHR. 11 One of the most significant achievements of the Convention is its enforcement system, in the form of the European Court of Human Rights. This court governs alleged breaches of the rights and freedoms granted by the ECHR. Like the Universal Declaration of Human Rights, the ECHR balances the protection of rights and freedoms, including respect for personal privacy, and justifiable restrictions to those rights and freedoms.12

Another important source are the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Organisation for Economic Cooperation and Development (OECD). This document was created in the 1980s, and it sought to harmonize national legislative frameworks on data protection among countries that cooperate within the organization. Even more importantly, the Guidelines introduce a set of principles and in this way further previously enshrined rights and freedoms concerning personal privacy and personal data protection. Also during the 1980s, the Council of Europe adopted the Convention for the Protection of Individuals regarding Automatic Processing of Personal Data (known as Convention 108). Convention 108 was a legally binding instrument in all countries that signed it. This Convention was opened for signature not only to Council of Europe states but also to all other countries outside of Europe. The additional significance of this document lies in its narrower scope (it focuses on protection with regard to processing personal data by automatic means). Convention 108 contains three parts: substantive law provisions that are mainly similar to the provisions contained in the OECD Guidelines, rules on the trans-border flow of data, and mechanisms for assistance and consultation. The convention protects personal data in a more elaborate manner than had been the case before. In this sense, it provided a foundation for the further development of data protection law.

The first initiatives from EU institutions for harmonizing national data protection legislation emerged in the mid-1970s. In that period, the European Commission called on the European Parliament to prepare a directive proposal that would harmonize national laws. The European Commission viewed Convention

12 Ibid, art 10(2).
108 as a benchmark for the broadening of principles regarding the non-automatic processing of personal
data.\textsuperscript{13} Almost 20 years after the first initiatives, in 1995, the Data Protection Directive was adopted (The
Directive).\textsuperscript{14} The Directive can be viewed as a valuable source for both the harmonization of national data
protection legislation and its improvement. However, its main flaw relates to the fact that the proposed
rights and obligations can be interpreted differently by different national legislative frameworks. The
transposition of the Directive’s principles into national legislation has brought about variations in legal
matters related to personal data protection. Such a state has affected, \textit{inter alia}, legal certainty, the
provision of cross-border services and financial transactions.

In the 2000s, the institutional perspective of the EU was strengthened through the adoption of The
Charter of Fundamental Rights\textsuperscript{15} and The Treaty of Lisbon.\textsuperscript{16} In general, the essential goal of these acts
was to improve the structure of the EU and to increase its effective functionality. Both acts enshrine core
values of personal data protection. The Charter’s most important contribution is its proclamation of the
right to personal data protection as a fundamental right. The Treaty of Lisbon serves as a legislative
standpoint for introducing a common legal framework in many fields striving towards the unification of
national legislation among EU Member States.

The historical progression of legislative protection of personal data established a need to further develop
the field in the early 2010s. In addition, the new socio-economic landscape generated by the progressive
development of new technologies shaped another set of reasons for improving personal privacy and
personal data protection. The emerging technologies have increased the cross-border exchange of goods
and services in the EU. For that reason, industries have an interest in the unification of EU Member State
legislation in order to remove the unnecessary administrative obstacles faced by businesses (obstacles
that ultimately maintain growing exchange rates).

Since 1995, the world has changed dramatically. Internet use and the development of telecommunication
services have resulted in data processing on a large scale. Today, the online environment is a suitable
ecosystem for successful business activities and everyday communication among people. Phenomena

\textsuperscript{13} Sian Rudgard, ‘Origins and Historical Context of Data Protection Law’ in Eduardo Ustaran (ed) \textit{European Data
\textsuperscript{14} 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 [1995] OJ
L281/31.
\textsuperscript{16} Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community,
such as web-based companies and social media platforms have already assumed a stable position on “the plateau of productivity.” Many emerging technologies have been climbing toward “the peak of inflated expectations” in an incredibly short period of time. However, many of these are already at the “through of disillusionment.” Increased technology production rates continue to generate more data to be processed, and hence misuse of the internet and the overall online ecosystem is far greater than it was in the 1990s (when the Directive was adopted).

Tech giants offer their incredible services apparently free of charge. Nevertheless, every activity in the online environment creates potentially lucrative information. Thus, chasing data collection and identifying opportunities for extracting useful patterns from the huge amount of available data are both our current reality and our current challenge. In addition, the new reality has shifted relations between the law, democracy and the rule of law. Tech giants can misuse their corporate function, position, wealth and know-how to affect policymaking. Moreover, their services can be used for quite dubious purposes that eventually realign the balance of political power, access to justice, morality, and general reasoning. Finally, national states can also misuse emerging technologies at the cost of human rights and freedoms.

For these reasons, in 2009 and 2010, the European Commission initiated a review of the state of personal data protection in EU Member States. Following a long, comprehensive review process, the Commission proposed reform of the Directive, which was to be replaced by a unique set of rules. Negotiations on the regulation text between the European Commission, the European Parliament and the Council of the EU lasted four years. In May 2016, the GDPR was formally adopted, and it became fully enforceable two years later.

2. The GDPR – Key terms
The GDPR is a comprehensive and extensive source of law (with 99 articles and 173 recitals). Article 4 of the GDPR provides a definition of the purpose of the regulation. For the purposes of understanding this study, explanations of the key terms of the GDPR are provided below.

**Personal data** is any information relating to an identified or identifiable individual (the data subject), irrespective of how and where it is contained. Any information that is clearly about a particular person constitutes that individual’s personal data. An individual is identifiable when, although he or she has yet to be identified, it is possible to do so by combining different pieces of information (identifiers) relating

---

17 For more info on “the plateau of productivity,” “the peak of inflated expectations,” and the “through of disillusionment,” please see: Gartner Hype Cycle <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle> accessed 15 July 2019.
to him or her. Although there is no definitive list of categories of personal data, we can organize types of data as follows:

- internal (beliefs, knowledge, preferences),
- external (identifying, ethnicity, sexual, behavioral, demographic, physical characteristics, medical),
- historical (life history),
- financial (account, ownership, transactional, credit),
- social (professional, criminal, public life, family, social network, communication).^{18}

**Data processing** is a GDPR concept that relates to anything an entity can do to or with personal data, either automatically or manually. Sending promotional emails, storing IP addresses, posting a photo of a person on a social network, arranging travel, shredding documents that contain personal data, video recording, payroll administration and almost anything else you can think of are examples of personal data processing.

A **data controller** is anyone (a person, a company, a public authority) who decides (alone or together with others) which pieces of personal data will be collected, for what purpose, for how long, for whom, and so forth. An employer, a hospital, a school, Facebook, Twitter and many other entities that have control over pieces of personal data can be considered data controllers.

Data controllers must be open about all facts relating to personal data processing and must provide comprehensive privacy information. The controller is responsible for taking care of the security of personal data and is liable if a data breach occurs. A data controller is also a go-to location if a data subject wishes to exercise granted rights.

A **data processor** is anybody (an individual, a company, a public authority) who processes personal data on behalf of the controller and upon its instructions. The controller may decide to outsource data processing activities as part of a service agreement. A processor will therefore need to process personal data to provide a required service to the controller. For instance, a marketing automation platform will need to process the names and emails of a retailer’s customers to send customized newsletters on the retailer’s behalf.

---

Whenever a processor is appointed, a written agreement, a so-called Data Processing Agreement or DPA) must be in place. This obligates the processor to apply the adequate measures to secure the controller’s data and to obey all other relevant data protection requirements.

**Data subject consent** is the most common legal ground for lawful personal data processing. According to the GDPR, data subject consent is “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she by a statement or clear affirmative action signifies agreement to the processing of personal data relating to him/her.”

Thus far, the development of EU data protection regulation has deployed many explanations about the structure, conditions, cases and general understandings of how and when the indication of someone’s wishes might be considered legitimate consent. European regulators are constantly analyzing and developing the notion of consent. However, we should be aware that the progressive development of emerging technologies and their role in personal data processing affect the shape of consent and present a challenge to legal and IT experts.

Although consent is one of the most disputable legal notions today, lack of data subject consent (or lack of other legal grounds) for lawful personal data processing may lead to considerable legal problems and fines.

A **personal data breach** occurs when the data for which a data controller/processor is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity. If this occurs and it is likely that the breach poses a risk to an individual’s rights and freedoms, the data controller/processor must notify the supervisory authority without undue delay. This should be accomplished within 72 hours of discovery of the breach. In addition, a data processor must notify the data controller and data subjects of any data breach that poses a high risk to the individuals affected.

The **Article 29 Working Party (Article 29WP)** was an advisory body established by the Directive. It was composed of representatives of data protection authorities from each EU Member State, the European Data Protection Supervisor and representatives of the European Commission. This body provided expert opinions on data protection issues and the application of the Directive. In addition, the Article 29WP raised

---

19 General Data Protection Regulation, art 4(11).
awareness of data protection and related rights. This body was replaced by the European Data Protection Board, formally established by the GDPR.

3. GDPR principles in detail
Certain principles lie at the heart of the GDPR. They are set out at the start of the legislation and inform everything that follows. They do not constitute hard and fast rules but rather embody the spirit of the general data protection regime. Compliance with the spirit of these key principles is therefore a fundamental building block for proper data protection practice. It is also key to compliance with the detailed provisions of the GPDR. Article 5 of the GDPR enshrines the following principles:

1. Lawfulness, fairness and transparency,
2. Purpose limitation,
3. Data minimization,
4. Accuracy,
5. Storage limitation, and
6. Confidentiality and integrity

Each of these principles is considered in further detail below in order to explain its core value and function, as well as its implementation in practice.

3.1 Lawfulness, fairness and transparency
The first principle is composed of three separate principles. Therefore, this section contains three separate subsections, each devoted to one pillar of the first GDPR principle.

3.1.1 Lawfulness
The first principle, lawfulness, states that personal data should be processed only if a data controller has a legal ground for doing so. Therefore, data processing must be carried out within the limits of applicable law. “Applicable law” refers not only to data protection legislation but also to other laws that regulate various areas, such as employment relations, health, taxation, the prosecution of crime, or any other area relevant to the general public interest. In short, personal data processing is considered lawful if it is in accordance with applicable law. The GDPR enshrines the following legal grounds, which can be applied to ensure the lawful processing of personal data:

- **Consent** - the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- **Contract** - the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- **Compliance** – the processing of personal data is necessary for compliance with a legal obligation to which the controller is subject;
- **Vital interests** - the processing is necessary to protect the vital interests of the data subject or of another natural person;
- **Public interest** – the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- **Legitimate interests** – the processing is necessary for the purposes of 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, in particular where the data subject is a child.\(^\text{23}\)

### Data subject consent

Data subject consent is likely the most common legal ground for ensuring the lawful processing of personal data. It is defined as “any freely given, specific, informed, unambiguous indication of the data subject’s wishes by which he or she, by statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”\(^\text{24}\) Consideration of the definition reveals that data subject consent contains four distinctive (and obvious) features:

- it must be freely given;
- it must be specific;
- it must be informed; and
- it must be indicated unambiguously.

### Freely given consent

One of the basic features of the data controller’s accountability lies in the fact that the controller should be able to demonstrate that the obtained consent has features of freely given consent. There are several specific situations worth mentioning in this regard.

\(^{23}\) General Data Protection Regulation, art 6(1).
\(^{24}\) General Data Protection Regulation, art 4(11).
First, the GDPR indicates that consent should not be relied on where there is a clear imbalance of power between the data subject and the controller. The relation between employer and employee is commonly cited as an example in this regard: because of the imbalance of power inherent in this relation, demonstrating that the data subject (the employee) has freely given his or her consent to the controller (the employer) becomes problematic. The employee’s subordinate position may raise doubts about whether he or she is genuinely able to withdraw his or her consent without suffering negative consequences. Employers should therefore rely on consent as a legal ground for the lawful processing of employees’ data only in very limited circumstances.

Second, consent is given freely only if the data subject’s autonomy is respected. Having genuine choice ensures the data subject’s ability to refuse or withdraw consent. Relying on a lower standard than genuine choice can result in invalid consent. In short, a data subject must be given a genuine choice to withdraw consent without any negative consequences.

Third, the declaration of consent should be separated from terms and conditions of other kinds. The reason for this requirement is that integrating a consent declaration in (or rendering it indistinguishable from) other issues (e.g. general terms and conditions for the provision of the service) may result in the data subject’s not being properly informed about the processing of his or her personal data, thus jeopardizing the validity of the freely given consent. Additionally, controllers should be cautious about the claim that consent is necessary for data processing as part of performing a contract. When assessing whether consent has been freely given, special attention should be paid to whether the performance of a contract is conditional on the data subject’s consenting to the processing of his or her personal data when such processing is not necessary for the performance of the contract.

Finally, the granularity of consent should be respected in order to preserve the consent’s validity. The requirements for granular consent are closely connected to the requirements of specific consent, which are discussed in the following subsection.

---

25 General Data Protection Regulation, recital 43.
28 Hordern (n 26) 120.
29 General Data Protection Regulation, art 7(4).
Specific consent
The second requirement for the validity of consent refers to “specific consent.” In order to comply with the requirement of “specific consent,” the data controller must apply: “(i) purpose specification as a safeguard against function creep, (ii) granularity in consent requests, and (iii) clear separation of information related to obtaining consent for data processing activities from information about other matters.”

Specific consent empowers transparency and user control. The data controller has an obligation to explain the intentions related to the use of the data in order to obtain the data subject’s consent to use the data for those purposes. In the case of multiple processing purposes, consent should be given for all of the relevant purposes. Nevertheless, consenting to data processing for multiple purposes might be problematic if a data controller cannot precisely explain and present all processing purposes. Consent should be obtained in a timely manner, i.e. before the data processing starts. Thus the data controller should be able to present all processing purposes in the pre-consenting phase; otherwise, the validity of the consent becomes problematic. If new processing purposes emerge after the initial phase, the data controller should specify them and ask the data subject for further consent in order to lawfully process the personal data for those new processing purposes. With this said, there is an important exemption from this requirement, which concerns the processing of personal data for the purposes of scientific research.

Informed consent
The next condition for valid consent refers to “informed consent.” In general, the data subject should be supplied with all relevant details about the processing activities. Articles 13 and 14 of the GDPR list the minimum scope of the information that must be provided. In addition, information should be given in a form such that the data subject can understand the necessary details of the processing of his or her personal data. To this end, the details should be presented in language that the data subject can understand. The use of opaque language containing complex terminology and legal jargon conflicts with the requirement of informed consent. A consent declaration text should be easily accessible, i.e. the terms and conditions to which a data subject consents should not be hidden on a webpage that is difficult to access. Nevertheless, in cases where there is limited space for the presentation of information, in order

---

30 Article 29 WP guidelines on consent (n 27) 11.
31 Hordern (n26) 120.
Unambiguos presentation of consent
The GDPR requires that a data subject give his or her consent via a clear, affirmative act. Thus, consenting should not leave room for doubt regarding the data subject’s intentions. An active motion or declaration is necessary for valid consent. Ticking a selection box can be considered an active motion, whereas pre-ticked opt-in boxes or tacit consent cannot. Consent obtained through intimidation, coercion or duress cannot be considered valid. Valid consent covers cases where a data subject selects the relevant technical parameters for an information society service. When selecting these parameters, the data subject should be provided with a clear indication of the context in which he or she is accepting the proposed data processing. Nevertheless, data controllers should design consent mechanisms in a manner that is clear to the data subjects. In addition, controllers must ensure that the giving of consent can be distinguished from other actions (e.g. the acceptance of a contract). Finally, consent should be given in a timely manner, i.e. before the controller initiates data processing operations.

Contract
The following legal ground for the lawful processing of personal data refers to the performance of a contract to which the data subject is party. The GDPR provides that the processing of personal data is lawful if it 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 before entering into a contract.” In its opinion on legitimate interests, the Article 29WP provides several details about processing personal data for the performance of a contract. The opinion states that there are two different scenarios in which processing personal data for the performance of a contract can be considered lawful. The first scenario is when the processing in question is necessary for the performance of a contract to which the data subject is party – for instance when the processing of a data subject’s address is necessary for the delivery of goods purchased online, as well as the processing of credit card details necessary for effectuating payment. Another example is the processing of gamblers’ financial data: the legal ground for the lawful processing of a gambler’s

32 Article 29 WP guidelines on consent (n 27) 14.
33 Ibid, 15.
34 Hordern (n26) 120.
35 Article 29 WP guidelines on consent (n 27) 17.
36 General Data Protection Regulation, art 6(1)(b).
38 Ibid, 16-18.
financial data for the indicated purpose is the performance of the gambling contract. The Article 29WP opinion on legitimate interests states that “it is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective.” Thus, the opinion emphasizes the importance of the connection between the assessment of necessity and compliance with the purpose limitation principle.

The second scenario concerns the processing of data that takes place before the parties have entered into a contract. This scenario covers pre-contractual relations, “provided that steps are taken at the request of the data subject, rather than at the initiative of the controller or any third party.” This includes cases where an online gambler must deposit funds into a personal account created for the purposes of gambling prior to engaging in that gambling. In this case, processing financial data so as to deposit funds (e.g. to transfer money from one bank account or credit card to a personal account formed for gambling purposes) can be considered a pre-contractual relation made at the request of the data subject.

Compliance
The next legal ground for the lawful processing of personal data is compliance with mandatory legislation. In order to lawfully process personal data, the data controller must comply with any relevant mandatory laws that impose an obligation to engage in such processing. For instance, if a piece of mandatory gambling legislation requires the implementation of a certain registration procedure, the data controller is required to use that procedure when registering its data subjects.

Vital interests
The protection of the vital interests of the data subject or of another natural person as a legal ground for the lawful processing of personal data “should in principle take place only where the processing cannot be manifestly based on another legal basis.” In particular, this legal ground applies in relation to the lawful processing of data only if such processing “is necessary to protect an interest which is essential for the life of the data subject or (…) of another natural person.” The interpretation of a data subject’s vital interests should be very restrictive and in general refers to “life and death” situations.

---

39 Ibid, 17.
40 Ibid.
41 Ibid, 18.
42 Dusan Pavlovic, ‘Online gambling in the EU: from data protection to gambler protection’ (Doctoral thesis, Tilburg University 2018)
43 Ibid, 175.
44 General Data Protection Regulation, recital 46.
45 Ibid.
Public interest
The processing of personal data in the service of the public interest is a legal ground for lawful personal data processing. The use of this legal ground for data processing must have a basis in EU law or Member State law.47 However, the data subject has the right to object to having his or her personal data processed on this ground. Once an objection has been made, the controller must interrupt further processing unless the controller “demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subjects.”48 Under the same conditions, the data subject has a right to object to having his or her personal data processed if the data controller bases the processing on the final legal ground listed above – legitimate interests.

Legitimate interests
The legitimate interests of a data controller or third party may be relied on as a legal ground for the lawful processing of personal data.49 The concept of an “interest” is closely related to the concept of a “purpose,” as enshrined by the Directive and the GDPR.50 However, an interest can be perceived as a “broader stake that a controller may have in the processing.”51 More importantly, a controller or third party’s interests must be legitimate in order to serve as a legal ground for the lawful processing of data. The inclusion of the concept of legitimacy refers to the fact that data controllers’ and third parties’ interests should not override the fundamental rights and freedoms of the data subject.52 The data subject’s rights and freedoms must be weighed against the data controller’s interests in order to determine whether those interests are legitimate.53

The opinion of the Article 29WP on legitimate interests proposes several elements that must be considered when this balancing of interests is carried out. The weighing process should examine the legitimacy of the interests in question and thus establish whether it forms a legal ground for the indicated purposes.54 The Article 29WP opinion on legitimate interests provides that controllers should not be able to claim a legitimate interest in the processing of personal data in order to unduly monitor the online and offline activities of individuals or to combine vast amounts of customer data “from different sources that

---

47 General Data Protection Regulation, recital 45.
48 Ibid, art 21(1).
49 Ibid, art 6(1)(f).
50 Article 29 WP opinion on legitimate interests (n 46) 24.
51 Ibid.
52 General Data Protection Regulation, art 6(1)(f).
53 Pavlovic (n 42) 183-184.
54 Ibid.
were initially collected in other contexts and for different purposes.” Therefore, the purpose limitation test is an integral part of balancing legitimate interests.

3.1.2 Fairness
Fairness with regard to processing personal data concerns the consequences of data processing. This principle states that the data controller should not process personal data in a way that negatively affects the data subject. Nevertheless, this idea should be approached with care, namely in situations where personal data is processed without the data subject’s being aware. In the case of a traffic offence, for example, the police department and the relevant court may process the personal data of the individual who committed the offence even without his or her knowledge. Processing the offence is not likely to affect the data subject in a positive way. Nevertheless, in this hypothetical example, despite the adverse effects of processing the personal data, the overall process is justifiable and hence complies with the fairness principle.

Fairness in data processing also concerns the idea that the data subject should be aware of the relevant aspects of processing his or her personal data. Awareness of the relevant facts allows for informed decision-making regarding the processing of personal data and data protection rights. Therefore, the principle of fairness is directly linked to the principle of transparency.

3.1.3 Transparency
Transparency is deeply embedded in EU law and promotes citizens’ trust in the processes that affect them. Transparency helps citizens to understand the relevant processes and contributes to fairness. In the context of the GDPR, transparency obliges data controllers to be open and clear towards data subjects when processing personal data. The GDPR regulates the minimum level of information on the processing of personal data that data controllers must provide to data subjects. With regards to the scope of this information, the GDPR distinguishes between data that is obtained directly from the data subject and data that is provided by other sources. In addition, the mode of communication with the data subject is regulated. Article 12 outlines the main elements of transparency. In particular, it defines the rules with which the data controller must comply when informing the data subject of his or her accompanied rights:

---

55 Article 29WP opinion on legitimate interests (n 46) 26.
56 For more on this, please refer to the section on the purpose limitation principle.
58 General Data Protection Regulation, art 13-14.
- information must be concise, transparent, intelligible and easily accessible;
- clear and plain language must be used;
- the requirement of clear and plain language is of particular importance when providing information to children;
- information must be in writing or by other means, including where appropriate, by electronic means;
- where requested by the data subject, it may be provided orally; and
- it must be provided free of charge.\(^6^0\)

The requirement regarding the provision of “concise and transparent” information “means that data controllers should present the information/communication efficiently and succinctly in order to avoid information fatigue.”\(^6^1\) In practice, this means that privacy-related information should be presented separately from non-privacy-related information. “Intelligible” information is information that can be understood by the average member of the intended audience. For that reason, this requirement is closely connected to the requirement to use clear and plain language. Complex language that is difficult to understand should be avoided. In addition, the linguistic structure of the information should not leave room for interpretation. With this said, there is no widely accepted template for how information should be structured and presented. Data controllers should therefore assess their audiences in order to present privacy-related information such that the relevant content can be understood by the average audience member. Taking into account Recital 39, which states that “natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data,” privacy related information must ensure that the data subject understands the main aspects of the processing of any personal data that relates to him or her. The requirement that the information be “easily accessible” entails that the data subject should not have to seek it out.\(^6^2\)

The default position for informing (or communicating with) data subjects is that the information be provided in written form.\(^6^3\) Nevertheless, information might be provided “by other means, including, where appropriate, by electronic means.”\(^6^4\) Thus, communication and the provision of information need not necessarily come in written form. Using visualization tools or a combination of visualization (e.g. icons,

\(^{61}\) Ibid, 7.
\(^{62}\) Ibid.
\(^{63}\) General Data Protection Regulation, art.12(1).
\(^{64}\) Ibid.
video clips, flowcharts, infographics) and text is recommended. Audio (oral) delivery of the information is desirable if the information is provided through screenless devices with audio capabilities. It is worth mentioning that it is preferable to use a layered approach when presenting the information. Nevertheless, the information should be easily accessible on a single location. Finally, the information must be provided free of charge, which means that access cannot be conditional.

3.2 The purpose limitation principle
The purpose limitation principle states that the data controller should process personal data only for specified, explicit and legitimate purposes. In other words, personal data should not be further processed for purposes that are incompatible with the controller’s original purposes. These primary purposes should therefore be considered limitations that the data controller must respect when processing personal data. The Article 29WP examined different elements and requirements regarding purpose limitation. These requirements are separated into two building blocks: “purpose specification” and the “compatible use test.”

3.2.1 Purpose specification
Purpose specification is “a prerequisite for applying any other data quality requirement.” The main function of purpose specification is to set boundaries for how data controllers can process personal data. A data controller must be clear about the purposes for which the personal data is being processed. These purposes must be documented and specified. The specification of purposes must be given “prior to, and in any event not later than, the time when the collection of personal data occurs.” Clear specification means that the data controller should “determine what kind of processing is and is not included within the specified purpose.” Thus, having a vague or general purpose may conflict with the purpose limitation principle. Responsible gambling purposes may be considered too general insofar as there are various mechanisms of responsible gambling. The specification of purposes must be precise, but it is preferable

---

65 Article 29WP guidelines on transparency (n 60) 25.
66 Ibid, 7.
67 General Data Protection Regulation, 5(1)(b).
69 Ibid, 11.
71 Article 29WP opinion on purpose limitation (n 68), 15.
72 Ibid.
that it not be too long or too difficult to understand. Concise and user-friendly information is preferable to the comprehensive presentation of purposes for which the data will be processed.

Purposes are made explicit when they are “clearly revealed, explained or expressed in some intelligible form.” Explanation should not leave room for doubt about the purpose of the processing or be difficult to understand. For that reason, the cultural and linguistic characteristics of the data subjects and other stakeholders relevant to processing the personal data should be taken into consideration. Making the purpose of the personal data processing explicit not only affects the predictability of data processing but also promotes the transparency principle. The requirement that purposes be made explicit also allows data subjects to make informed choices.74

Finally, the third part of purpose specification concerns legitimate purposes. This requirement directly corresponds to the first GDPR principle (lawfulness).

3.2.2 The compatible use test
The second building block is known as the “compatible use test.” This test is used in case-by-case assessments of whether the further processing of the data is compatible with the initial processing purposes.75 Alongside formal assessment is substantive assessment, which serves to identify both the new and the original purposes of processing the data in question, “taking into account the way they are (or should be) understood, depending on the context and other factors.”76 In relation to carrying out compatible use tests, Article 29WP proposes the following elements for consideration:

- the relationship between the purposes for which the data has been collected and the purposes of further processing;
- the context in which the data has been collected and the reasonable expectations of data subjects as to their further use;
- the nature of the data and the impact of its further processing on data subjects; and
- the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.77

73 Ibid, 16.
74 Ibid, 17.
75 Ibid, 21.
76 Ibid.
First, the relationship between the initial purpose and the purposes of further processing should not be seen as a mere linguistic matter. As mentioned above, what is essential is the relationship between the purposes for which the data was initially collected and the purposes of further processing it. In some situations, the further processing “was already more or less implied in the initial purposes or assumed as a logical next step in the processing according to those purposes.” In addition, there is the possibility of partial connections (or a lack of connection) between original and further purposes. Thus, the proximity of original to further purposes should be taken into consideration. Where the distance is greater, it will be more difficult to pass the compatible use test and to satisfy the requirements of the purpose limitation principle. It must be stressed that assessment of the relationship is quite contextual and should observe the common perceptions of the main stakeholders involved in data processing.

The second issue of the compatible use test refers to the context in which the personal data was collected and the reasonable expectations of the data subjects regarding its further use. Therefore, it concerns what a reasonable person in the data subject’s situation would expect about the processing of his or her personal data in that context. In order to answer this question, the nature of the relationship between the controller and the data subject should be examined. This examination should review not only the legal aspects of the relation but also the relevant customs and common practices in that context. Additionally, the balance of power between the data subject and the data controller, as well as the legal grounds used to meet the criterion of lawfulness, should be investigated.

The third factor concerns the nature of the data and the impact of further processing on the data subject. This is particularly important for protecting individuals against excessive and improper processing of their personal data. The nature of the data is particularly relevant to conducting the compatible use test. It is important to be aware of whether the processed data belongs to special categories of data. Such data is specifically protected, and thus it is reasonable to expect that the further use of special categories of data will be closer to the original purposes. In general, when assessing the impact of further data processing, all potential consequences (both negative and positive) should be assessed. Where the predicted consequences are negative or uncertain, it is less likely that further data processing will pass the compatible use test.

---

79 Ibid.
80 Ibid, 24.
Finally, the fourth factor of the test refers to safeguards applied by the controller to ensure fair processing and to prevent any undue impact on data subjects. Implementation of the appropriate technical and organizational measures should ensure data protection and security. This is important for maintaining the integrity and confidentiality of personal data. Accordingly, data integrity and confidentiality will be distinguished as separate principles and presented in sub-section six of this section.

3.3 Data minimization

The essence of the data minimization principle is the notion that the data controller should process the minimum scope of personal data in order to fulfil the purpose of data processing. The data controller should therefore determine the minimum amount of personal data and keep (process) only that amount. In addition, the accountability principle requires that the data controller be able to demonstrate that only this minimum amount of data will be processed. The data minimization principle is linked to the data accuracy principle and the storage limitation principle. These three principles are known as data standard principles.81

In general, personal data should be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”82 However, there is no explicit definition of what constitutes adequate, relevant and limited data in the GDPR. There are, however, expert opinions on this. What counts as adequate, relevant and limited data is context dependent. The specific purposes of personal data processing should be taken into account when assessing the adequacy, relevance and limitation of data. Therefore, whoever makes this assessment should be aware of the needs related to data processing. The UK Data Protection Authority (hereinafter the ICO) takes into consideration the characteristics of different groups of data subjects in order to determine the data that should be processed. Closely connected to the storage limitation principle, the ICO stresses that data should be reviewed regularly and deleted when it is not necessary for the intended purpose of the processing. In addition, the processing of data that contains irrelevant details will breach this principle.83

The European Data Protection Supervisor states that “[t]he principle of ‘data minimisation’ means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is

82 General Data Protection Regulation, art. 5(1).
83 ICO (n 81)
necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it.”  

Concerning proportionality, data controllers should therefore take into account the amount of data to be collected. Collecting an excessive amount of data (relative to the purposes of the data processing) without restriction is considered disproportionate. A “save everything” approach therefore conflicts with the data minimization principle.  

Recital 39 states that “personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.” Thus, the data controller should assess various means of processing personal data and choose a method associated with the fewest adverse consequences for personal privacy.

In practice, the implementation of the data minimization principle can be either problematic or straightforward. Again, this depends on the context of the personal data processing. In some cases, a simple assessment is sufficient to satisfy this principle, whereas in others a complex, multidisciplinary system of assessment will be necessary.

3.4 Data accuracy

Implementation of the data accuracy principle should ensure that personal data is accurate, kept up to date and erased or rectified when it is inaccurate. The GDPR does not define what accurate data consists in. As a rule of thumb, however, accurate data is data that is not misleading or incorrect. The correctness of the data should correspond to the purpose of processing it. It should accurately represent the data subject and his or her relationship to the data controller. In addition to being correct, the data must be complete. The data can be considered complete when its processing fulfils the predefined purposes of the data processing. For instance, the identification of a gambler is conducted properly if certain predefined documents are checked. In such a case, processing data from alternative documents might also serve to identify the gambler, but the identification will be incomplete so long as the relevant documents are not checked. Some documents do not provide complete information about the individual in relation to the purpose of processing the data (in some cases, having the subject’s name and residential address is sufficient for identification, whereas in others processing a personal identification number in addition to the subject’s name and address will be necessary). Finally, the last element of data accuracy refers to its value. Data that does not serve the purpose of the processing has no value in this context.

---

85 Filippidis (n 57) 110.
86 General Data Protection Regulation, recital 39.
Thus, it does not have significance. Significance may relate to the monetary context; useful data has financial value in certain markets. In addition to monetary significance, however, data can have legal significance, and this can entail that the data should be treated differently.

Similarly, accurate and inaccurate data should be treated differently. The GDPR ensures that every reasonable step should be taken to rectify or delete inaccurate data. The ISO adds that the status and source of personal data must be clear, that any challenges to the accuracy of information should be carefully considered, and that the information should be updated regularly.

Taking reasonable steps (or measures) should “be understood as implementing processes to prevent inaccuracies during the data collection process as well as during the ongoing data processing in relation to the specific use for which the data is processed.” For this reason, the purpose for which the data is processed and the nature of the data should be considered in order to maintain data accuracy. Inaccuracy with regard to personal data may be the consequence of improperly verifying the authenticity of the information. Thus, data controllers must evaluate the reliability of the data source. Moreover, additional care should be taken when possible data inaccuracy can have adverse consequences for the data subject.

Data accuracy generates data controller accountability with regard to responding to requests, on the part of data subjects, to rectify personal data. In particular, the GDPR grants the data subject “the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.” Thus, the data subject has “the right to have incomplete personal data completed, including by means of providing a supplementary statement.”

---

88 General Data Protection Regulation, recital 39.
91 Filippidis (n 57) 111.
92 General Data Protection Regulation, art 16.
93 Ibid.
In sum, the implementation of the data accuracy principle involves maintaining (ensuring) data accuracy prior to data collection and during the ongoing processing. Additionally, data accuracy may be the consequence of the data controller’s obligation and the data subject’s right to rectification.

3.5 The storage limitation principle

Storage limitation is the last of the three principles that shape data standards. The key point of this principle is that the data controller should not keep data longer than is necessary for the purposes of the data processing. Once data is no longer necessary for further processing, it should be deleted. Data can be kept longer only if doing so serves the public interest of archiving, scientific or historical research, or statistical purposes, so long as appropriate technical and organizational measures are put in place. This principle directly correlates to the principles of data minimization and data accuracy. Having clear policies about data deletion decreases the possibility of irrelevant and/or inaccurate data and the excessive processing of such data. Additionally, retaining data for longer than necessary in relation to the predefined purpose of the processing increases the risk of the data’s being processed unlawfully due to a potential lack of legal ground.

From a practical point of view, storing large amounts of data without conducting a data cleansing procedure may come with unnecessary costs and threats related to data security. In addition, where more data is collected than is necessary, there may be problems in responding to a data subject’s request to access personal data or to fulfil obligations related to the data subject’s right to be forgotten.

The data controller should determine the period for which the data will be stored. If this is not possible, then criteria for determining the retention period should be defined. Article 30 states that the data controller should generate a record of its processing activities. These records should include, *inter alia*, “where it is possible, the envisaged time limits for erasure of the different categories of data.” However, it is not always easy to determine the appropriate data retention period. Therefore, there is no strict obligation to determine an exact period of data retention for every set of data (the data might be categorized according to its nature, the data subject, the purpose of processing it, or any other criteria),

---

94 General Data Protection Regulation, art 5(1)(e).
96 Ibid.
98 General Data Protection Regulation, art 30(1)(f).
but having standards for reviewing and deleting data should be a part of any data retention policy. Therefore, data controllers should be able to justify reasons for retaining data for a stated period, taking into consideration the purpose of the processing.

Retention periods may vary not only for different sets of data but also due to different legal requirements. There are various legal requirements for keeping certain types of data (for instance, AML legislation imposes an obligation to retain gamblers’ data for a certain period of time; employers often have to keep records of ex-employees in order to comply with labor law requirements).

As stressed above, the data should be deleted upon the expiration of the retention period. This can be done in several ways and on various levels. Different types of data require different deletion procedures (e.g. the process for deleting hard copy data differs from that of deleting digital data). The deletion of digital data is complex and can come in different forms. Making data unavailable can count as deleting it, but there are also further levels of deletion. Data may be made unavailable to certain audiences while remaining accessible to others (e.g. database administrators). Thus, only the erasure of data from all databases and backups can ensure complete deletion.

### 3.6 Confidentiality and integrity

The importance of the confidentiality and integrity principle is captured metaphorically by the notion that “the data protection principles are the celebrities of the data protection world,” such that “security is always on the A list, a true VIP.”

99 The general favoring of one principle over others is not desirable insofar as the particular context can give priority to certain principles. This notwithstanding, it cannot be denied that neglecting the confidentiality and integrity principle can erode the overall system of personal data protection or make it meaningless. Thus, it is reasonable to ask why this principle deserves a special place in the hierarchy of GDPR principles. The answer hinges on two considerations.

First, a data security risk is not a standalone risk. If personal data is compromised, many other data subjects’ rights that derive from other GDPR principles will also be jeopardized. If personal data is stolen, for example, data controllers and processors cannot make guarantees about the purposes for which the compromised data will be used. In addition, stolen data is likely to be processed for purposes to which the data subject has not agreed. Therefore, linked to breaches of the purpose limitation principle, this

constitutes an unlawful processing of personal data that is additionally non-transparent and likely unfair to the data subject. Breaching the confidentiality and integrity principle is clearly a serious legal risk.

The second reason refers to reputational risk. If a data controller/processor uses weak technical and/or organizational measures to ensure the security of personal data and consequently incurs a data breach, this will probably affect its corporative identity. Such a scenario may result in a reduction of customer trust and ultimately in negative business development.

3.6.1 The essence of the principle
The GDPR regulates the principle of integrity and confidentiality as the requirement that personal data 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.”

Data integrity is usually described in terms of maintaining the accuracy and consistency (validity) of the data during its lifecycle (e.g. between updates of the data record). Respecting data integrity requires that the data be modified only by authorized persons. Thus, to preserve the integrity of the data, the following actions are necessary:

- preventing unauthorized subjects from making modifications;
- preventing authorized subjects from making unauthorized modifications, such as mistakes; and
- maintaining the internal and external consistency of objects so that their data is a correct and true reflection of the real world and any relationship with a child, peer, or parent object is valid, consistent, and verifiable.

Virus attacks, unauthorized access, and various intentional and unintentional mistakes can affect data integrity. For instance, when an unauthorized entity is allowed to decrypt encrypted data, the integrity of the data is jeopardized. In this case, the data is physically available, but its content is useless for further processing.

Data confidentiality can be defined as a “practice of making sure that private information is kept secret.” Data must be protected from unauthorized access, use, and disclosure while in storage, in process, and

---

100 General Data Protection Regulation 5(1)(f).
in transit. Data confidentiality can be jeopardized by various types of intentional and unintentional violations. Capturing network traffic, stealing passwords, social engineering, port scanning, shoulder surfing, eavesdropping, and sniffing are just a few examples of activities that can affect the confidentiality of personal data.\textsuperscript{104}

The integrity and confidentiality principle states that only authorized people may manipulate the data within the scope of their authorization in order to preserve it in an accurate and complete state in relation to the purpose of processing it and in order to keep the data accessible and usable.\textsuperscript{105} The integrity and confidentiality principle is often equated with the data security principle, which concerns the protection of network and information systems from attack. However, the GDPR involves not only the security principle but information security. The information security principle is a broader term that covers the application of physical security and organizational security measures.\textsuperscript{106}

The GDPR obliges both data controllers and data processors\textsuperscript{107} to protect personal data through the entire lifecycle of the data processing. The obligation to ensure secure data is not new, but the GDPR stipulates that specific measures must be implemented. With regard to shaping data protection by design and default\textsuperscript{108} and the security of data processing,\textsuperscript{109} the GDPR identifies specific technical and organizational measures that should be included in any information security framework:

- 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;

---

\textsuperscript{104} Stewart, Chapple and Gibson (n 102) 60.
\textsuperscript{107} Although Article 5 is neutral concerning who should implement appropriate technical and organizational measures, Article 32 clearly states that both controllers and processors are obliged.
\textsuperscript{108} General Data Protection Regulation, art 25.
\textsuperscript{109} General Data Protection Regulation, art 32.
a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.\textsuperscript{110}

The implementation of these measures usually requires multidisciplinary engagement, mainly by legal and technical information security experts. Nevertheless, human capacity is just one of several types of resources necessary for carrying out appropriate information security measures. The data controller/processor should settle on a specific budget in order to meet these requirements. However, since the funds and capacities available to controllers/processors and the context of data processing differ from case to case, it is reasonable to wonder what an acceptable, legal set of measures and their implementation would look like from a legal point of view. The answer might lie in the fact that, rather than requiring absolute security, legislators often require a merely appropriate level of security when it comes to personal data.\textsuperscript{111}

### 3.6.2 Appropriate, not absolute security

The relevant provisions of the GDPR require the implementation of appropriate security when it comes to protecting personal data, namely taking into “account 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” in order to determine the appropriate technical and organizational security measures. Thus there is no “one-size-fits-all” solution.\textsuperscript{112} Different contexts require different implementation measures. Data controllers who process special categories of data should implement higher security measures than data controllers who process personal data that does not significantly affect the rights and freedoms of the data subject. In addition, data controllers/processors are expected to assess risk by taking into account not only the nature of the data that is to be processed but also the threats, vulnerabilities, exposure, and safeguards in place.\textsuperscript{113} Higher exposure, serious threats and vulnerabilities should affect decisions about organizational and technical

---

\textsuperscript{110} General Data Protection Regulation, art 32(1)(a)(b)(c)(d).


\textsuperscript{113} A threat is an action or inaction that might result in “accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.” Vulnerability relates to the weakness of a safeguard of countermeasure. Exposure relates to being susceptible to personal data because of a threat. Thus, exposure refers to the possibility that a vulnerability can or will be exploited by a threatening agent or event. A safeguard, or countermeasure, removes or reduces a vulnerability or protects against one or more specific threats. For more on this, see: Stewart, Chapple and Gibson (n 102) 146-148.
security measures. Therefore, risk assessment should consider human factors, security management, the physical and technological environment, any applicable policies and controls, and business process frameworks.

It is not difficult to see that high-level risks regarding personal data processing generate a need for strong safeguards and the implementation of highly protective security measures. Apart from the assessment of internal capabilities to ensure data security and potential (external) threats, proper decision-making on information security frameworks includes consideration of the “state of the art” concerning data security practices and facts related to the costs of their implementation. In general, data controllers and processors should consider industry best practices, not just average industry practices.114 However, it is not easy to determine what counts as “industry best practices.” This is generally decided on the basis of reasonably informed professional opinions about appropriate security measures in particular circumstances and is thus a matter of consensus.115 Finally, implementation costs should not preclude industry best practice. With this said, there is no single established stance regarding the budget that must be devoted to security measures. It is therefore important to stress that security mechanisms are designed to protect data against specific kinds of threats (for instance, adversaries with specific technical capabilities). In other words, it is not necessary to design security systems such that they are protected against all threats. Such an effort would be prohibitively expensive and likely ineffectual. Proper human capacity is thus the core of any security system; risk assessment should be undertaken properly in order to accurately determine risk factors and to design appropriate measures. In this way, budgets for security measures can be created according to the real data protection needs of the situation.

114 Room (n 111) 172.
115 Ibid.
Part Three – A Typology of Self-Exclusion Mechanisms

1. What is a self-exclusion mechanism?
Acceptable gambling involves balancing human freedoms, responsibilities and choices that may lead to negative effects. Gamblers bear the brunt of the responsibility for their actions, and thus the ultimate decision to gamble belongs to the individual. The notion that this decision represents a choice is one of the main principles of many scientific models of responsible gambling. Developing the Reno model, Blaszczynski et al. describe responsible gambling in terms of a set of principles, policies and practices designed to prevent and mitigate potential gambling-related harms, including problem gambling. Notwithstanding the criticism levied against this principle, a gambler’s personal decision remains the focal point of responsible gambling. In general, responsible gambling is composed of various elements that are aimed at promoting consumer protection, community/consumer awareness and education about gambling-related harms, as well as access to effective treatment. An omnipresent measure for implementing responsible gambling and preventing problem gambling is the use of self-exclusion mechanisms.

Gamblers who think they are spending too much time or money on gambling or are concerned by other aspects of their gambling behavior may use self-exclusion tools to exclude themselves from gambling activities for a certain period of time. The registration of excluded online gamblers in databases helps to ensure that online gamblers who willingly exclude themselves will not be allowed to gamble for a period of time that they themselves determine. Self-excluded gamblers are legally banned from gambling, and online gambling service providers should not ignore this fact. Respecting a self-exclusion request often also includes the interruption of gambling-related commercial communication during the period of self-exclusion. Operators may be found legally liable if they permit self-excluded online gamblers to gamble.

---

117 Ibid 308.
118 Gerda Reith criticizes this principle by claiming that it is a reflection of neoliberal ideas about responsibility that derive from the neoliberal concept of the minimal state, the reduced role of external governance and the exaggerated importance of individual self-control. For more on this, see Gerda Reith, ‘Reflections on Responsibility’ (2008) 22 Journal of Gambling Issues 149.
119 Ibid.
Because the gambling legislations of EU Member States have yet to be harmonized, the regulation of self-exclusion mechanisms is characterized by legislative diversity. Nevertheless, the application of self-exclusion mechanisms is part-and-parcel of responsible gambling, and it would not be incorrect to say that it is an inseparable part of online gambler protection. In practice, however, there are many obstacles to the effective implementation of self-exclusion mechanisms; in particular, the diversity of national legislative frameworks concerning the implementation of this mechanism often impedes the cross-border provision of online gambling services. In addition, service providers that operate in the same national market rarely exchange data on self-excluded players. Finally, identification management with regard to the identities of online gamblers can differ among national markets and jurisdictions, and thus the cross-border exchange of data on self-excluded gamblers risks being ineffective. Taking into consideration the availability and accessibility of the personal data that needs to be processed for the purposes of identifying self-excluded online gamblers and regulating self-exclusion mechanisms, a detailed explanation of the organization of self-exclusion mechanisms is presented in the following section.

2. Identification and regulation as cornerstones of self-exclusion

In everyday life, identification refers to a set of processes related to the disclosure of information about a person and the use of that information. Certain pieces of information about a person, such as his or her name, date, place of birth, citizenship and identification number(s) constitute identifiers that are commonly used to distinguish that person from others. Identification can be described as a process that reveals data connected to personal identity. Explaining the notion of personal identity, Nabeth focuses on a twofold perspective. The first can be referred to as the “process perspective” of personal identity, the meaning of which resembles a widespread understanding of identification – the use of the most common identifiers in order to find out who someone is. The second is the “structural perspective” of identity, which views identity as a set of attributes that characterize the person in different contexts and activities. Pfitzmann and Hansen define identity as “any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons.”

122 Ibid.
identification within a group. The utilization of a set or subset of these attributes and relevant identifiers serve the purpose of identification.124

Knowledge of the “structural perspective” of a gambler’s identity is very important for responsible gambling. The structural perspective of a gambler’s identity might indicate personal features in certain contexts – for instance gambling behavior patterns, including those that indicate a problematic relation to gambling. In registration for self-exclusion purposes, online gamblers usually reveal their full name, nationality, email address, residential address, personal identification number, and username, and thus the identification of a self-excluded online gambler primarily concerns the “procedural perspective” of an online gambler’s personal identity. Revealing this perspective is fundamentally important for recognizing self-excluded online gamblers and preventing them from gambling during the period of self-exclusion. Thus, for this purpose, processing permanent data (e.g. biological characteristics, place and date of birth) is more reliable than processing more temporary markers (e.g. address, email address and features of personal behavior).

The effective identification of self-excluded online gamblers depends not only on the type of data being processed for registration purposes but also on the accessibility and availability of the data. The level of data accessibility and availability depends on the regulation of self-exclusion mechanisms. Regulatory arrangements for self-exclusion mechanisms vary from self-regulation to regulation at the national, international and supranational level. Regulations may limit data processing mechanisms in a manner that affects the accessibility and availability of self-exclusion databases. Thus, for the purposes of this paper, self-exclusion mechanisms are distinguished according to two dimensions – horizontal and vertical. Although these dimensions are intertwined, for presentation purposes the horizontal dimension concerns the connectivity among self-exclusion databases. Connectivity affects the accessibility and availability of gambler data, which further influences the effective identification of self-excluded online gamblers. The vertical dimension concerns the existence of regulations aimed at organizing self-exclusion mechanisms. Taking into consideration both dimensions and their practical variations, self-exclusion mechanisms can be constructed in the following ways:

- horizontally disconnected; vertically unregulated
- horizontally connected; vertically unregulated

- horizontally connected; vertically regulated
- horizontally disconnected; vertically regulated

2.1 Horizontally disconnected; vertically unregulated

Horizontally disconnected and vertically unregulated self-exclusion mechanisms are not connected (on the horizontal dimension). Online gambling service providers who manage these kinds of self-exclusion databases leave them at the disposal of their consumers. Moreover, only representatives of the service provider can access these databases. In practice, this means that service provider A will be allowed to access its own database of self-excluded gamblers (database A) but not the list of self-excluded gamblers on database B (which is managed by service provider B). The second crucial characteristic of this mechanism concerns self-regulation (the vertical dimension). Competent national legislation may (or may not) enshrine the obligation that every licensed service provider ought to organize and maintain a self-exclusion mechanism. However, if a national gambling law contains a general obligation without the specified organizational and functional features of a self-exclusion mechanism, this system cannot be considered vertically regulated.

Online gambler registration in this kind of database enables the gambler to exclude him or herself from a particular type of game or from all of the games offered by the service provider. The main duty of online gambling service providers in this regard is to reliably identify those customers who have willingly excluded themselves from gambling and who have therefore requested that they not be allowed to gamble for a determined period of time. If a self-excluded gambler is still able to gamble, several risks may arise. Gamblers may exacerbate their already undesirable gambling behavior and prompt problem gambling. In such a hypothetical case, service providers (and/or subjects who manage self-exclusion databases) may be liable, and gamblers may initiate a judicial trial in a competent forum. There have been few court decisions regarding responsibility in relation to the organization and maintenance of self-exclusion mechanisms. With this said, Calvert v. William Hill Credit Ltd, decided in the United Kingdom,125 is worth mentioning in this regard.

125 Calvert v. William Hill Credit Ltd [2008] EWCA Civ 1427.
The claimant, Mr. Calvert, was a compulsive gambler. He was aware of his destructive and uncontrollable gambling behavior, which had led to the loss of a substantial part of his wealth. Recognizing this, he asked William Hill to exclude him for six months from any further gambling. However, the employee who was in charge of managing William Hill’s register of self-excluded players did not take the necessary steps to ensure that the exclusion was complete and functional. Therefore, Mr. Calvert was allowed to continue gambling. He did so using William Hill’s services and was ruined himself financially by losing almost two million GBP while self-excluded. Mr. Calvert initiated a claim against William Hill, claiming negligence in the duty of care to refuse self-excluded players from gambling. He claimed the overall amount of funds lost during the self-exclusion period. What is interesting is that the court decided against Mr. Calvert’s claim, finding that William Hill was not responsible for the financial damage incurred by Mr. Calvert. According to the court’s findings, Mr. Calvert had already been a pathological gambler before he excluded himself from William Hill’s services and could have chosen many alternatives to gambling services with which to gamble and thus bring about his financial ruin.
It is beyond the scope of this study to discuss whether service providers should be held responsible for the losses incurred by self-excluded players in such cases and the arguments supporting the Court’s decision in the Calvert case. What is important is that the Court’s decision in this case points out the main weakness of horizontally disconnected, vertically unregulated self-exclusion systems. Self-excluded players in such cases limit themselves from engaging in the services of only one service provider. But there are always other service providers available on the market. Hypothetically, if this system of self-exclusion were the only one available, then any gambler who wanted to fully exclude him or herself from all possible gambling options would have to initiate self-exclusion processes with all applicable licensed gambling service providers (and unlicensed service providers too, if accessible on the market). Such a self-exclusion system would be more protective if there were a monopoly on the provision of online gambling services or if just a few operators were licensed and accessible.

One of the main features of this self-exclusion mechanism is based on self-regulation. Self-regulation might enable the broad autonomy of service providers in decisions about whether to accept the registration of gamblers from different countries. Under the presumption that service providers should not discriminate on the basis of citizenship or residency in the registration process, service providers ought to make the self-exclusion mechanism available to all registered online gamblers. Therefore, this system of self-exclusion should not be limited to gamblers from certain countries (typical of self-exclusion systems that are vertically regulated) but should be made available to all registered gamblers.¹²⁶

### 2.2 Horizontally connected; vertically unregulated

The second type of self-exclusion mechanism is based on collaboration between service providers. Service providers are horizontally connected in a way that enables them to exchange data about self-excluded gamblers. In general, this type of mechanism is composed of several databases of self-excluded players. Each company in the group of connected companies has its own register of self-excluded players that should be available to the other companies. Therefore, each of the connected companies has access to the others’ databases when determining whether a customer is allowed to gamble.

This type of self-exclusion mechanism enables self-exclusion not merely from the gambling services offered and provided by one operator but from the gambling services offered by all connected companies. If a gambler has three different accounts at three connected operators that organize and manage three different self-exclusion registers (one register per operator), then his or her registration in one database

¹²⁶ Pavlovic (n 42).
of self-excluded gamblers will activate the self-exclusion mechanism for all three; all three service providers will be bound by the gambler’s self-exclusion, regardless of where it was requested.

Diagram 2 – Horizontally connected; vertically unregulated self-exclusion mechanism

Within this type of mechanism, there is an additional subcategory: it is also possible for several online gambling service providers to manage a unique database of self-excluded gamblers. This database would contain personal data available to all connected companies. For instance, if three different but connected online gambling service providers manage a unique database of self-excluded players, a gambler’s registration in this database is a sufficient step towards activating the self-exclusion mechanism for all three connected online gambling service providers. A distinctive feature of this subcategory is the fact that there is no data exchange among service providers; there is only a data transfer between a central database and service providers.

Cooperation among service providers enables interoperability in relation to self-exclusion data. This factor refers to the horizontal connectivity of self-exclusion mechanisms. The lack of a legislative requirement for the exchange of self-exclusion data reveals that such a system is not regulated vertically. Like the first
type of self-exclusion mechanism (which is neither horizontally connected nor vertically regulated), mandatory legislation may oblige service providers to develop and offer self-exclusion mechanisms as a responsible gambling measure. However, in this case it is still the service provider who decides on the form that this mechanism will take. For that reason, there is cooperation among service providers that ensures a level of interoperability between databases, based on agreements made between service providers (and not because of national or international legislation).

Again, the positive side of vertically unregulated self-exclusion systems is that they are self-regulated. National gambling legislations may limit cooperation among service providers by obliging them to exchange gambler data only with operators that are formally licensed in particular national jurisdictions. For this reason, systems that are vertically unregulated enable cooperation and data exchange among service providers that are licensed in various jurisdictions (or not licensed at all).

Although interoperability between databases is one of the core characteristics of horizontally connected mechanisms, the vertical dimension in this type of system can present several challenges to the effective functioning of the mechanism, especially if the databases of self-excluded online gamblers are managed by service providers licensed in different countries. First, data protection legislation in different countries can regulate data processing and the transfer of data in different ways. This can give rise to difficulties concerning issues of legal compliance. Secondly, non-harmonized national legislations can impose different technical standards concerning the registration and identification of gamblers and regarding information security issues. Data may be transferred to national systems with lower security standards, thus exposing that data to information security risks. This issue becomes particularly complex when the self-exclusion mechanism is based on several interoperable databases managed by several service providers, each licensed in different national states. Finally, it is also possible for a particular type of game to be legal in one national market and illegal in another. Therefore, gamblers should at least be aware of the service providers and the types of games that will be inaccessible for the agreed period of self-exclusion and, conversely, which service providers and games will remain accessible.\textsuperscript{127}

2.3 Horizontally connected; vertically regulated

A horizontally connected and vertically regulated mechanism of self-exclusion can appear at two different levels. The first concerns vertical regulation at the level of the nation state. The second concerns vertical regulation at the international or supranational level. The main difference concerns the entities (state,

\textsuperscript{127} Ibid.
international or supranational organizations) that create and enforce the applicable regulations. Regardless of whether we are concerned with vertical regulation at the national, international or supranational level, the main feature of this mechanism is cooperation between service providers licensed in states that are members of international or supranational organizations. In this type of mechanism, regulations at the national, international or supranational level oblige all relevant service providers to engage in the exchange of data. This means that all service providers licensed in a particular state must exchange self-exclusion data among themselves (as is the case with mechanisms organized at the national level) or with service providers licensed in other states that are members of the relevant international or supranational organization.

The interoperability among databases containing self-exclusion data is the main feature of horizontal connectivity. This aspect is not significantly different from the other case of horizontally connected self-exclusion mechanisms. Rather, the difference here concerns the regulatory aspects that are related to the vertical dimension. This is important in relation to organizational aspects concerning the functionality of vertically regulated self-exclusion mechanisms. The organization of data exchange should be regulated in ways that enable effective database interoperability. In other words, it would be strange to create a mandatory self-exclusion mechanism that was horizontally connected and vertically regulated at the supranational or international level if states or members of the organization lacked harmonized standards for the technical infrastructure that is necessary for the proper functioning of the self-exclusion mechanism. For instance, if Italy, Spain, and France decided to harmonize their gambling legislation in order to enable the effective exchange of self-exclusion data, they would, *inter alia*, have to harmonize their procedures and standards for registering gamblers. A similar claim might be made with regard to mechanisms organized at the national level – the standards must be harmonized in order to enable effective data exchange among online gambling service providers.
The current lack of harmonization with regard to technical standards may lead to problems related to the registration and verification of consumers’ personal data. The main problems will be related to the accurate identification of self-excluded gamblers and privacy concerns. The registration of consumers in one state might be based on the processing of certain personal data that differs from that in another country. In such a case, certain difficulties with regard to the identification of self-excluded gamblers from different countries might arise. In addition, certain challenging security issues also emerge in vertically regulated and horizontally connected systems of self-exclusion. On the one hand, considering that all service providers must be allowed access to the data of all self-excluded players, regardless of where the data is stored, high-level security measures (which are potentially not harmonized among service providers or entities that manage self-exclusion databases) could hinder effective access. On the other hand, an “easily accessible” approach would expose databases, potentially making them desirable targets for cybercrime actors.
The main advantage of this type of mechanism is the possibility of excluding oneself from the services offered by a large number of online gambling operators. Moreover, by using this mechanism, these exclusions are obligatory for all service providers licensed in at least one country (vertical regulation at the state level) or even in several countries (the international or supranational level). Therefore, from an organizational perspective, service providers must check all registered self-excluded players in the state (or states) before providing their services. This solution can be problematic where there are dozens or even thousands of licensed service providers in one state. It is more manageable where there are few service providers, however.

Allowing for the exchange of data only among licensed online gambling service providers presents a challenge of another sort. It is hard to believe that operators whose services are accessible but who operate without the required national gambling license for the provision of gambling services would be included in a national self-exclusion mechanism, since it is organized and managed by the state, which issues the gambling licenses. With a vertically unregulated self-exclusion mechanism, it is up to service providers to decide on which operators will be included in the joint self-exclusion system. Therefore, even unlicensed operators may participate in horizontally connected (but vertically unregulated) mechanisms.

Concerning the vertical dimension of vertically regulated self-exclusion mechanisms, however, it is reasonable to assume that unlicensed operators will be considered formally illegal and because of this will not be allowed to participate in the system.

Exchanging data with unlicensed service providers can be useful from the perspective of responsible gambling. This situation risks opening a Pandora’s box of complex legal problems and dilemmas, however, such as whether something that is useful should be vitiated by something that is illegal; questions as to the relative importance of protecting gamblers (by enforcing self-exclusion mechanisms) and protecting the public interest (the general goal of national law); and questions as to which legal sources have greater significance (national law or international and supranational obligations). Thus, the harmonization of national regulations on gambling-related issues should be carried out to ensure the proper functioning of this sort of self-exclusion mechanism.128

2.4 Horizontally disconnected; vertically regulated

A horizontally disconnected but vertically regulated mechanism is the last form of self-exclusion in the typology proposed in this study. Like the previous form, this kind of self-exclusion mechanism can be

128 Ibid.
organized at the national, international or supranational level. The difference here is in the lack of data exchange between service providers. In contrast to the first form (horizontally disconnected and vertically unregulated), however, the vertical regulation of this system does require some form of jurisdiction-wide check as to whether a gambler has excluded him or herself. Therefore, instead of relying on the horizontal exchange of data, the mechanism here can rely on a central database of self-excluded online gamblers that service providers ought to check.

In Spain\textsuperscript{129} and Denmark\textsuperscript{130} self-exclusion mechanisms are implemented at the national level. These registers are administrated by national gambling authorities and contain data on all registered gamblers in Spain and Denmark who wish to exclude themselves from gambling online. The main advantage of

\textit{Diagram 4 – Horizontally disconnected; vertically regulated self-exclusion mechanism}


\textsuperscript{130} For more on the Danish register of self-excluded gamblers, see: Spillemyndigheden, ‘Rofus’ \texttt{<https://spillemyndigheden.dk/en/rofus-exclusion-gambling>\textgreater} accessed 16 July 2019.
vertically regulated national self-exclusion mechanisms is the opportunity to exclude oneself from the games offered by all online gambling service providers licensed in the state that administers the self-exclusion mechanism. From an organizational perspective, mechanisms that are not horizontally connected are easier to form and operate than horizontally connected ones. Horizontally connected mechanisms are composed of a large number of channels for the exchange of data (each service provider needs to establish the communication channels necessary for the exchange of self-exclusion data with all of the service providers that legally operate in a particular system), whereas with horizontally disconnected mechanisms each service provider must only establish a channel with the central database. Therefore, horizontally disconnected (but vertically regulated) mechanisms are thought to be more effective than those that are horizontally connected. In addition, the inclusion of a state authority (or an international or supranational organization) may promote trust in the proper functioning of the relevant self-exclusion mechanism. With this said, a single central database may be more vulnerable to hackers than several databases within horizontally connected self-exclusion systems. Furthermore, insofar as each service provider must be able to communicate automatically with the central database, standards for data exchange must be established and followed.

*Diagram 5 – Horizontally disconnected; vertically regulated self-exclusion mechanism (regulation on international or supranational level)*
Apart from the mechanisms organized at the national level, vertical regulation can involve central databases of self-excluded online gamblers that are operated and managed by a supranational or international body. Because online gamblers can also be offered services by operators licensed in foreign jurisdictions (an operator licensed in one country but available in others), an effective supranational or international register of self-excluded gamblers could enable better protection than other types of self-exclusion. The practical implementation of this system would be quite difficult, however, and it will probably never see the light of day. Due to political and regulatory issues, there is no international or supranational organization that could be in charge of this task. Nor is it likely that such an organization will be established in the near future. It is hard to believe that national states would create an international or supranational organization in charge of gambling issues, the regulations of which would have priority over national rules.\footnote{Pavlovic (n 42).}
Part Four – When the GDPR Meets Self-Exclusion Mechanisms

This part identifies the strengths and weaknesses of the above-presented self-exclusion mechanisms. In the following sections, the principles referred to above are analyzed in the context of applied types of self-exclusion mechanisms. This part also presents the accountability principle, which summarizes the main measures that data controllers must put in place in order to comply with GDPR principles.

1. Lawfulness, transparency and fairness
The first GDPR principle ensures the lawful, transparent and fair processing of online gamblers’ personal data. As explained in Part Two, there are several legal grounds for lawful data processing. The determination of the legal nature of gambling-related activities, including self-exclusion, affects the lawfulness of online gamblers’ personal data processing.

One of the main conditions for the lawful provision of online gambling services is the registration of the gambler. This is a necessary step which, once completed, authorizes a person who intends to gamble online to use the services.\textsuperscript{132} The registration process can be carried out in several ways, but in general it serves to verify the gambler’s age and to satisfy other requirements related to the responsible provision of gambling services.\textsuperscript{133} First, registration allows for the confirmation of whether a consumer is permitted to gamble. Second, it ensures the legality of the conclusion and realization of the gambling contract (or contracts). In other words, after having completed the registration process, online gamblers can conclude gambling contracts with the online service provider. Following a successful registration process, several actions must be conducted to conclude a lawful gambling contract (e.g. depositing funds and placing a bet). In addition, online gambling service providers must check the databases of self-excluded gamblers in order to preserve the legality of the gambling contract. Checking the online gambler data revealed during the registration process and then again disclosed when a gambler excludes him- or herself is a \textit{conditio sine qua non} of the valid conclusion of a gambling contract. Thus, a contract regarding the provision of online gambling services is illegal (void or nullified) if the customer has not already been registered and if the relevant self-exclusion databases have not been checked. For this reason, the registration process can be viewed as a form of interference by the state (as a third party) or other regulatory bodies in the relationship between the gambler and the gambling operator. By imposing mandatory registration, a regulator constrains the autonomy of the contractual parties’ wills and in this

\textsuperscript{132} Ibid.
\textsuperscript{133} Ibid 83–85.
way shapes the conditions involved in offering and accepting a gambling contract. Therefore, it might be said that the registration procedure belongs to the domain of contractual relations and serves to preserve the legality of the performance of a gambling contract.\textsuperscript{134}

Processing online gamblers’ personal data is necessary for the performance of a gambling contract (to which the data subject, an online gambler, is party). In addition, registration processes may be taken as a form of data processing that takes place before the parties have entered into a contract. We should remember, however, that the Article 29WP opinion on legitimate interests states that “it is important to determine the exact rationale of the contract, i.e. its substance and fundamental objective.”\textsuperscript{135} Thus, it might be reasonable to question whether processing self-exclusion data is really necessary for the conclusion and performance of a gambling contract. Given that in certain European countries the self-exclusion mechanism is stipulated and is not an obligatory measure for the purposes of responsible gambling, it seems that checking databases listing self-excluded players is not a “taken-for-granted” legislative requirement that must be met in order for the conclusion and performance of a gambling contract to be legal. In particular, horizontally connected and vertically regulated self-exclusion mechanisms may include online gambling service providers that are licensed in jurisdictions where gambling laws do not require self-exclusion mechanisms. By contrast, in countries where self-exclusion is mandatory (and hence checking the databases of self-excluded players is obligatory), compliance with legal obligations might also be used as a ground for the lawful processing of data. In vertically unregulated systems, on the other hand, entities (included in the system) are able to decide whether (and how) to implement self-exclusion systems. For that reason, alternative legal grounds for the lawful processing of self-excluded online gamblers’ personal data must be discussed.

Protection of the vital interests of the data subject is not a possible legal ground for the lawful processing of self-exclusion data (insofar as it is applicable only in “life and death” situations). In addition, promotion of the public interest cannot be considered a legal ground for the lawful processing of self-exclusion data. It would be very hard to prove that preventing self-excluded players from gambling serves directly as a protective measure for maintaining the public interest.

The data subject’s consent is the most used (and most discussed) legal ground for the lawful processing of personal data in the online ecosystem. In general, consent is shaped in various ways by different fields of law. According to the author’s hands-on experience, online gamblers must often accept terms and

\textsuperscript{134} Ibid.

\textsuperscript{135} Ibid 17.
conditions and privacy statements when they carry out the registration process. The validity of this consent can be problematic, however. Most of the problems with the valid consent given by online gamblers concerns their ability to express their free will and to understand what is going on when their personal data is being processed.

When it comes to informed consent, there are two types of requirements. The first concerns the quantity of information, the second the quality of the information. The information should be structured in a way that enables the data subject to understand the process of data processing. Thus, the data subject should be aware of the consequences of said processing. People have different levels of knowledge, skill, and experience, however, and hence it is reasonable to ask how to create a set of information that serves to inform an ordinary gambler about the complexity of data exchange for the purposes of self-exclusion (especially when we are talking about horizontally connected mechanisms). Another problem concerns informing online gamblers about all necessary aspects of data processing. With horizontally connected mechanisms, it is possible for a large (or even unknown) number of service providers to process the self-exclusion data. Also, in vertically regulated and horizontally connected mechanisms where national legislations are not harmonized, we face the problem of informing data subjects not only of who is processing the data but also of how the data is processed (if we presume that different national legislative frameworks will set different requirements concerning how the data of self-excluded players must be processed). This hypothetical scenario poses challenges when it comes to satisfying the criteria of informed consent. Moreover, the data controller must evaluate the audience’s capacity to understand certain information. The GDPR does not enshrine conditions for guiding assessment of the data subject’s subjective characteristics, however. Moreover, the GDPR determines the threshold of information of which the data subject should be aware (the identity of the controller and the purpose of the processing).\(^\text{136}\) Insofar as the purpose of the data processing is obvious when a gambler excludes him or herself and the scope of the revealed data is known, there are no problematic issues concerning the requirements of specific consent. The situation is not so clear when it comes to freely given consent, however.

Recital 42 states that “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.” Regardless of type, self-exclusion mechanisms in general are meant to deprive online gamblers of their right to withdraw consent and their right to be forgotten for the period of self-exclusion. The use of self-exclusion mechanisms is an

\(^{136}\) General Data Protection Regulation, recital 42.
example of when a gambler limits his or her own opportunities to engage in gambling. Therefore, gamblers who exclude themselves restrict their own rights and freedoms. By doing so, they promote their personal autonomy (gambling restrictions are not imposed but self-initiated) and limit their own freedom to a certain extent (no gambling for a specified period) to prevent problem gambling and to promote their own wellbeing.\textsuperscript{137}

The final legal ground is legitimate interests. Behind the use of this ground for the lawful processing of personal data is a guarantee that the interests of data controllers and/or third parties will not override the fundamental rights and freedoms of the data subject.\textsuperscript{138} A balance must be struck between data subjects’ rights and freedoms and data controllers’ interests in order to determine whether those interests can be considered legitimate. Therefore, a balancing test should be carried out. The test evaluates the relation between the interests of the data controller or third parties and the interests of the data subjects. If the data controllers and/or third parties’ interests deserve more respect than the data subjects’ rights and freedoms, legitimate interest may serve as a legal ground for lawful data processing. Article 29WP proposes several elements to be considered for testing purposes.

The starting point for testing should concern the impact of data processing. The processing of self-exclusion data is clearly necessary to keep self-excluded online gamblers away from gambling for a certain period. Thus, processing this type of data can have a positive impact on gamblers. In vertically regulated systems, however, there are mandatory provisions that impose prohibitions on self-excluded gamblers. Therefore, there is a further ground for lawful data processing (compliance with mandatory legislation). In vertically unregulated systems, the situation may be different. A legitimate interest can be used as a legal ground, but this should be approached with caution. When processing self-exclusion data, the interests of the data controllers may serve a protective function. If we assume that this data will not be used for lucrative (and obviously conflicting) purposes (e.g. commercial communication), then the interests of the data subjects (to be protected from gambling-related harms) and those of the online gambling service providers (to protect their customers from gambling-related harms) may overlap. It is reasonable to wonder why online gambling service providers would take up this protective role (where there is no mandatory provision imposing it). The answer may be found in the operators’ desire to be socially responsible or to build a better corporate image (regardless of general skepticism regarding this explanation). However, if a gambling operator (or a group of operators) who values self-regulated,

\textsuperscript{137} Pavlovic (n 42).
\textsuperscript{138} General Data Protection Regulation, art 6(1)(f).
responsible gambling has a legitimate interest in processing the data of self-excluded online gamblers for the purposes of preventing them from gambling for a certain period, the following question arises: Is it legitimate to process self-exclusion data for purposes that go beyond the proper functioning of a self-exclusion mechanism in order to additionally contribute to responsible gambling? This is precisely the question that will be examined in the following discussion of the purpose limitation principle.

2. The purpose limitation principle
As explained in Part Two, personal data should not be processed for purposes that are incompatible with the purposes for which it was originally collected. In order to investigate whether the purpose limitation principle has been respected, data controllers must conduct purpose limitation tests that are in essence twofold tests – a purpose specification and a compatible use test in one. The requirement of purpose specification contributes to the transparency of personal data processing. The data controller or processor should be explicit and specific about the purpose of the data processing and may process the data only for legitimate purposes. Given that self-exclusion mechanisms are one of the most important measures of responsible gambling, a dilemma emerges concerning the compatibility of processing personal data from self-excluded gamblers and the additional purpose of preventing the occurrence of gambling-related harms, thereby contributing to responsible gambling. Attention to the compatible use test is crucial for resolving this dilemma.

Processing data on online gamblers’ behavior (including information about self-exclusion) can have a positive impact on gamblers. This positive impact may ground the legitimacy of the data controllers’ interests (and may justify the use of legitimate interests as a ground for lawful data processing). Nevertheless, erring on the side of caution, the compatible use test should serve as a case-by-case assessment of whether further processing is compatible with the initial purposes of data processing. In the case of self-exclusion, the initial purpose of the data processing (self-exclusion) may well be compatible with further purposes insofar as both promote moderate gambling. Nevertheless, we can question whether the data subject could reasonably expect the processing of his or her data beyond the purposes of self-exclusion. Reasonable expectation has not been clearly defined in EU law, and alternative legal institutions may serve as a theoretical niche for settling what counts as a “reasonable expectation” in certain contexts.140

139 The reasonable expectations of data subjects as to the further use of their data is a testing requirement (more on this in Part 2, subsection 3.2).
140 Pavlovic (n 42) 187-189.
If we generate a hypothesis in which a vertically unregulated system processes self-exclusion data for purposes that contribute to responsible gambling (even beyond the immediate purposes of self-exclusion), then the legitimate interests of the data controller (or processor) should be used as a ground for the lawful processing of data. It is clear that use of the data subject’s consent (obtained for self-exclusion purposes) to process data for further purposes beyond self-exclusion cannot ensure the lawfulness of data processing. For such further purposes, the data controller/processor should obtain separate consent (under the presumption that the purpose specification test fails). In vertically regulated systems, the relevant legislation may define situations in which self-exclusion data can be processed for further purposes. In these cases, separate consent would not be necessary insofar as compliance with mandatory laws serves as the proper legal ground for lawful data processing.

In sum, protecting the rights and interests of data subjects and ensuring that the interests of data controllers are legitimate requires engaging in a balancing of considerations that includes a purpose limitation component and a compatible use component. Determining the lawfulness of personal data processing by appealing to the legitimate interests of the data controller or a third-party is a double-edged sword, however. The application of this legal ground limits the autonomy of data subjects with respect to their decision to process their personal data. Therefore, there is a serious ethical question concerning whether vertically unregulated systems should have this type of discretion. Should we allow self-regulated service providers to play a paternalistic role in order to protect online gamblers? Moreover, should we trust vertically unregulated systems and give them the opportunity to process more data (or already obtained data) for seemingly compatible purposes. We cannot deny that restricting the autonomy of online gamblers (with regard to decisions about processing personal data disclosed during their gambling activities) may be beneficial to them. In theory, processing more data about risky gamblers may ultimately limit their gambling activities (and subsequently prevent gambling-related harms). This leads, to a further ethical question, however: Should we treat purpose limitation tests as outdated and open the door for the excessive processing of personal data for the good of data subjects?\textsuperscript{141} Answering this and the above questions is important for the further development of self-exclusion mechanisms, responsible gambling, and responsible innovation. These issues lie beyond the scope of this study, however, and thus belong to future research.

3. Data standards

It is often remarked that data is “the new oil.” It is indisputable that the general value of data has been increasing and that available technologies are capable of collecting and storing incredible amounts of data. A crucial problem facing the IT industry (and indeed all industries), however, is finding proper way to process data for its intended purposes. Big data is not only a phrase that describes a huge amount of information but also a mechanism capable of processing data for predetermined aims. In order to build the necessary infrastructure to extract data for useful patterns, the data that is meant to be processed must satisfy certain standards. Principles regarding data minimization, data accuracy and storage limitation continue to shape the standards of personal data processing.

As explained in Part Two of this study, the data minimization principle should prevent potential problems related to the scope of the processed data. The scope of the data depends on many factors, however, including regulatory requirements. With regard to vertically regulated and horizontally connected systems, problems can occur when the online service providers included in this system are based in different countries. Problems emerge when national states regulate the identification of gamblers in different ways concerning the scope and type of data that must be processed for the purposes of gambler identification. For instance, if the laws of state A require the processing of a gambler’s name, identification number and email address for identification purposes, and the laws of state B require the gambler’s email, social security number and residential address for the same purposes, then the common identifier is merely an email address. That is obviously insufficient for reliable identification. Therefore, where identification standards and determination of the scope and type of data that meet the data minimization principle are harmonized, service providers in horizontally connected systems that are vertically regulated will be challenged to process a broader scope of data (than is really necessary) in order to both reliably identify online gamblers and meet all national identification requirements. Even without harmonization, however, there is a solution that might serve to overcome the problems related to legislative fragmentation. In horizontally connected and vertically regulated systems, service providers included in the system can create their own systems for identifying gamblers. Such internal identification systems could be applied following the complete registration of a new gambler. Every newly registered gambler might be assigned a specific identifier developed only for identification purposes among service providers. Self-excluded gamblers could be identified by specific identifiers that are unique within the overall system. A double-identification system could satisfy national legislative requirements on the one hand and data minimization criteria on the other. Whereas there are alternative options for overcoming legislative fragmentation and ensuring the effectiveness of vertically regulated and horizontally connected
mechanisms, the situation is different when it comes to vertically regulated but horizontally disconnected mechanisms that are established at the international or supranational level. In this case, it is necessary to harmonize national laws on the identification of gamblers; otherwise, it will be almost impossible to maintain the effectiveness of this type of self-exclusion mechanism. In this system, there is no connectivity between service providers, and hence they cannot create an internal identification mechanism.

When we focus on vertically unregulated systems, self-regulation should ensure the reliable identification of gamblers and self-excluded gamblers. It is reasonable to presume that vertically unregulated mechanisms will be more suitable for organizing effective identification systems. Nevertheless, caution should be given to the scope of the data that can be requested for processing purposes. In any case, the harmonization and subsequent standardization of identification systems is necessary.

Horizontally connected mechanisms face concerns related to data accuracy. Whenever a service provider included in the group of companies that are horizontally connected receives a request to erase or rectify inaccurate information, this request must be communicated to all other companies in the group. In horizontally disconnected systems, this request is only addressed to service providers, and eventually to the entity that manages self-exclusion database (e.g. in case of vertically regulated but horizontally disconnected mechanisms). Horizontally connected systems must therefore organize data exchange effectively in order to ensure that the data remains accurate.

Finally, the retention of data is the last standardization principle. Data controllers should not keep data for longer than the processing requires. Given that the GDPR does not stipulate a strict period over which data should be kept, the data retention period must be determined by internal policies and/or national legislation. Self-regulation may determine the period for which the data will be retained. The service providers included in this system should determine the period of exclusion. Otherwise, all service providers should retain the relevant data until the longest period of self-exclusion expires. It would be pointless to have service providers included in vertically unregulated mechanisms determine different periods for self-exclusion. If service provider 1 were to set three months as a default period for self-exclusion, for example, while service provider 2 set six months, the foundations of horizontal connectivity would be undermined. From the broad perspective of responsible gambling, it would be ethically dubious for a service provider to permit someone to gamble (following the expiration of the relevant self-exclusion period) while that person was still self-excluded with other service providers. This kind of problem also affects vertically regulated systems at the international level. Again, as in many other matters, the
harmonization of standards is still the most desirable solution for the effective functioning of horizontally connected mechanisms.

It is reasonable to expect data to be erased after the period of self-exclusion has expired. In other words, if an online gambler has been self-excluded for six months, all data should be deleted as soon as those six months are over. Data may be kept longer, however, if there are legitimate interests that coincide with responsible gambling purposes.\footnote{More on this in section 2 of this part.}

4. Security and confidentiality

Although the GDPR stipulates certain organizational and technical measures as essential to the information security framework, there is no universally accepted guidance on how to organize critical infrastructure for data protection. The NIST framework for improving critical infrastructure cybersecurity\footnote{National Institutes for Standards and Technology, ‘Framework for improving Critical infrastructure Cybersecurity’ (2018) \url{https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf} accessed on 16 July 2019.} proposes an information security framework based on a process perspective. Organizations should be able to identify the business context, the accompanied risks, and the infrastructure they manage. They should develop protective measures, detect anomalies and defects, create response plans in case of security breaches and be capable of recovering the overall system. Apart from the NIST framework, there are other sources for developing industrial best practice for information security management. Although “industrial best practice” is an amorphic term that is interpreted in different ways, certain recommendations, standards and specifications are generally accepted. Their implementation is thus desirable and viewed not only as contributing to compliance with data protection regulation but also as essential to data governance. ISO standards (particularly package 27001),\footnote{As an international non-government organization, the ISO has a long tradition of providing standards that are recognized as guaranties of good practice, the application of which ensures quality, safety, and efficiency. More on this at: International Organization for Standardization, ‘All about ISO’ \url{https://www.iso.org/about-us.html} accessed 16 July 2019.} the ICS body of knowledge,\footnote{The ICS’s body of knowledge for the preparation of CISSP is worth mentioning insofar as a CISSP certificate is one of the most valued security certifications in the field of information security management. The body of knowledge for preparation for this certification contains almost everything needed to design, engineer, implement and run an information security program. More on this at: (ICS)\textsuperscript{2}, ‘CISSP – The World’s Premium Cybersecurity Certificate’ \url{https://www.isc2.org/Certifications/CISSP} accessed 16 July 2019.} and The European Union Agency for Network and Information Security (ENISA) publications\footnote{ENISA is a center of expertise for cybersecurity and is the most renowned European organization in the field. It provides hands-on experience, recommendations and policy implementation. Its publications are taken as relevant sources for the presentation of technical and organizational security measures. More on this at: European} have proposed valuable recommendations for the application of organizational and
technical measures. Therefore, for the purposes of this research, these sources have been taken as a benchmark for discussion of the technical and organizational measures that should be implemented to protect data confidentiality and integrity.

Given that one of the essentials of the GDPR is related to documentation management, an important part of security management is dedicated to security policy and procedures for the protection of personal data. A security policy should at least contain the roles and responsibilities of personnel, the baselines for technical and organization measures adopted for the security of personal data, and an indication of the data processors or other third parties involved in the processing of personal data. Persons in charge of specific security (including security officers) should be appointed, and formal documentation is recommended. Horizontally disconnected systems may have a single security officer, whereas horizontally connected systems should be expected to have at least one security officer per service provider. Each service provider included in this type of mechanism should appoint a security officer and define its duties and areas of responsibility. The role of each security officer should be clearly defined and separated from the duties of other security officers and from the duties and responsibilities of auditors and DPOs. This is necessary to prevent the unintentional or unauthorized processing of personal data.

It is preferable to have separate security policies regarding the processing of personal data related to self-exclusion. In horizontally connected mechanisms, the security policies and procedures adopted by each service provider should be harmonized in order to enforce similar technical measures and thus ensure the effective exchange of data. However, the application of similar technical security measures by a large number of data controllers might be perceived as a vulnerability. When technical security measures at one point in an overall system are compromised, all other points are also at risk (if we presume that cyber attackers will apply the same methodology to other databases within the system). When we are talking about security measures, we should recall that security should be not absolute but appropriate.\textsuperscript{147} Within horizontally connected mechanisms, there may be online gambling service providers with different internal organizations and capacities to implement technical and organizational measures. Thus, it is quite possible that more wealthy service providers will be expected to implement the latest emerging technologies (which might be very expensive), whereas moderate and smaller providers will implement appropriate technologies that they can afford. In any case, from the perspective of security management,


\textsuperscript{147} See Part 2, subsection 3.6.
technical security measures should be regularly reviewed, revised and upgraded. Where appropriate, ensuring the diversity of technical measures is welcomed, although this should not disproportionally hinder effective data exchange.

The most important part of security management is clearly determined, specific access control rights. An access control policy should contain detailed, appropriate access control rules,\textsuperscript{148} access rights and restrictions for specific user roles in the processes and procedures related to processing personal data related to self-exclusion. For instance, a responsible gambling manager might access this data to investigate how often certain gamblers have restricted themselves from gambling. An IT manager might access the same type of data in order to maintain security. It is preferable, however, to pursue strategies that prevent security managers from obtaining information about gambler self-exclusion while at the same time providing information that is useful for security protection. For this purpose, it is recommended that Privacy Enhancing Technologies (PET) derived from acknowledged standards and best practices in the field of data security be implemented during the development of projects that process personal data, including self-exclusion data. PET should be applied in a “cradle to grave” manner. In other words, specific technologies and techniques created to support privacy and data protection should be applied from the earliest to the latest phases of the development (realization) lifecycle.\textsuperscript{149}

Security management includes resource/asset management. Asset management should provide a clear view of assets associated with self-exclusion data and facilities that process this data/information. It might include hardware, software, networks, servers, workstations, and their locations. The complex process of data flow (particularly in horizontally connected mechanisms) should be mapped and described. Mapping data and explaining its flow is important not only for meeting the obligations of Article 30 of the GDPR but also for creating a basis for risk assessment. Asset management identifies not only personal data, however, but also other types of information and processing facilities insofar as breaches of various information can affect the protection of personal data. Accurate, regularly reviewed, consistent and aligned inventories are important prerequisites for risk management.\textsuperscript{150} In addition to providing

\textsuperscript{148} For instance, having technical security measures such as proper authentication mechanisms based on a combination of a password (with a high level of complexity) and username, supported by two-factor authentication. As a supportive measure, device authentication might help to increase the level of protection.
\textsuperscript{149} It is recommended that the relevant bodies conduct vulnerability testing and penetration testing through a trusted third party to find the balance between privacy protection and maintaining proper levels of security. In addition, it is advisable to carry out both broad and deep security testing.
information about which assets an organization possesses, inventories also provide information about ownership of those assets, the classification of data, its value, its criticality, and its sensitivity to unauthorized disclosure and modification.\textsuperscript{151}

Concerning used resources and assets, it should be stressed that they must provide an appropriate level of at-rest data and network/communication security. When we focus on horizontally disconnected systems, the primary focus should be on data at rest. With horizontally connected systems, network/communication security can often be perceived as largely significant. In horizontally disconnected systems, all data is stored in a single database, whereas in horizontally connected systems self-excluded data may be scattered around the world. Therefore, the security infrastructure surrounding the central database should be more critical (in the case of horizontally disconnected systems), insofar as the protection of data transfers is more critical in horizontally connected systems. There are several measures that can help to ensure at-rest data and network/communication security. The table below presents the most important measures proposed by ENISA:

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Data at rest</th>
<th>Network/Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Files and records should be encrypted through software (or hardware), including files and records on storage devices</td>
<td>Encryption through cryptographic protocols should be used</td>
</tr>
<tr>
<td></td>
<td>Full disk software encryption should be enabled on workstation operating system drives</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access control</th>
<th>Data at rest</th>
<th>Network/Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Database and application servers should only process the personal data that needs to be processed in order to satisfy the processing purposes</td>
<td>Access to the IT system should be controlled (with access given only to specific users followed by specific processes)</td>
</tr>
<tr>
<td></td>
<td>Authorized devices should be given access to the IT system</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th>Data at rest</th>
<th>Network/Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Where possible, workstations should not be connected to the internet</td>
<td>The information system network should be separate from other types of networks</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic monitoring/controlling</th>
<th>Data at rest</th>
<th>Network/Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Users should not be able to deactivate or bypass security settings</td>
<td>Traffic to and from the IT system should be monitored and controlled through firewalls and intrusion detection systems</td>
</tr>
</tbody>
</table>

\textsuperscript{151} Ibid 15.
Users should not have privileges related to installing or deactivating unauthorized software applications

The means of copying personal data from workstations to external devices should be disabled

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Anti-virus software should be configured and security updates should be carried out regularly</th>
<th>Firewalls and intrusion detection systems should be configured regularly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pseudonymization</td>
<td>Data should be pseudonymized through data separation</td>
<td></td>
</tr>
</tbody>
</table>

When data processing is carried out on behalf of the controller, the controller should use data processors that sufficiently guarantee the implementation of appropriate technical and organizational measures. Article 28 of the GDPR enshrines several requirements concerning the engagement of data processors. Processing personal data via processors should be governed by a contract (Data Processing Agreement) between the controller and the processor concluded prior to the commencement of processing activities. The processor should process personal data only in accordance with written instructions given by the data controller, and any transfer of data to third countries or the engagement of sub-processors must be permitted by the data controller. Thus, the data processor should establish the same level of personal data security as that which is mandated in the security policy of the data controller. This leads us to a further issue that reveals the importance of harmonizing security management in horizontally connected systems: namely the problem that if security management is not harmonized, it will be possible to include a data processor in an overall system whose technical and organizational measures do not meet the criteria of certain service providers. Where this occurs, such service providers will not be able to guarantee an optimal level of data security. In such a scenario, the risk of a data breach is higher.

Incident response and business continuity are the logical continuation of security management. If security management flaws result in a data breach, then proper incident response measures must be in place, as

---

152 General Data Protection Regulation, art 28.
well as an action plan that can ensure business continuity. Handling incidents, including personal data breaches, should be based on a response plan with detailed procedures for ensuring an effective and orderly response to incidents pertaining to personal data. Personal data breaches must be reported to the management, the relevant stakeholders, and the lead data protection authority unless that breach does not threaten the rights and freedoms of natural persons. Notification procedures for reporting such breaches to the competent authorities and to data subjects should be put in place and should follow Articles 33 and 34 of the GDPR. The documented incident response plan should include a list of possible mitigation actions and a clear assignment of roles. All incidents and personal data breaches including details about the event and subsequent mitigation actions, should be recorded.

In the event of an incident/personal data breach, a business continuity plan should be implemented. This plan should contain the main procedures and controlling mechanisms necessary for ensuring the required level of continuity and the IT system’s ability to process personal data following the incident. The plan should define the level of guaranteed service quality for the core business processes following the incident. Additionally, alternative facilities should be considered, depending on the organization and the acceptable downtime of the IT system.

5. Accountability
Accountability is a general legal principle and is often associated with liability and responsibility. In general, this principle refers to liability in civil law and to culpability in criminal matters. The GDPR introduces accountability as a new principle, and in general it obliges the data controller to be responsible for compliance with all other principles and to be able to demonstrate this compliance. Given that each principle has already been presented and discussed in the context of the functioning of self-exclusion mechanisms, this section outlines the most important measures and activities that data controllers should put in place:

- Data controllers should establish appropriate technical and organizational measures, including security measures;
- Data protection or privacy policies, as well as “cookie” policies, should be adopted and implemented;
- Appropriate legal grounds for lawful data processing should be obtained or ensured;

---

153 General Data Protection Regulation, art 33(1).
155 General Data Protection Regulation, art 5(2).
- A “data protection by design and default” approach should be implemented. In doing so, data controllers should take a privacy-preserving approach from the initial phases of project planning to the final phases of its realization;
- Data controllers should conclude contracts with organizations that process personal data on their behalf. Appropriate safeguards must be put in place for the transfer of data;
- Documentation about processing activities, including data inventories, should be developed and maintained;
- In case of a personal data breach, the necessary reports should be created and recorded;
- Data protection impact assessments for personal data processing should be carried out if such processing poses a high risk to the data subject’s interests;
- Data controllers should appoint a data protection officer;
- All relevant codes of conduct should be adhered to, and all certification schemes (where applicable) should be signed up to.

The accountability principle requires constant and ongoing compliance with all requirements laid down by the GDPR. Therefore, data controllers should review, update and where necessary upgrade all implemented measures. Privacy management should include not only the development and maintenance of measures but also activities that raise awareness of personal data and privacy protection. Finally, being accountable can both positively affect trust-building among consumers and mitigate enforcement action.156

Part Five – Conclusion

The identification of self-excluded online gamblers is crucial for their protection. Identification of these gamblers can be improved by extending the scope of available data and increasing data accessibility. To this end, interoperability between databases of self-excluded online gamblers is highly recommended. Processing the personal data of self-excluded online gamblers must satisfy data protection regulations, however, including the principles of the GDPR. GDPR principles shape the contours of such regulation, and all other rules and obligations derive from them. These principles impose requirements for the lawful processing of personal data. They oblige data controllers and processors not to process data for purposes that have not been agreed to (or are otherwise not permitted). GDPR principles create standards for processing data, imposing an obligation on controllers and processors to restrict the scope of their data processing to what is genuinely necessary for meeting predetermined purposes. In addition, data must be kept up to date and for a limited period. Finally, the principles provide instructions on how to preserve the integrity and confidentiality of personal data.

As we have seen, the demanding requirements of data protection are in tension with the impetus to process as much data on online gamblers as possible in order to promote responsible gambling. The legitimacy of both interests is indisputable, and hence striking the proper balance between them remains a challenge. Gambling regulations and data interoperability deserve particular attention when it comes to finding this balance. These factors therefore serve as two main pillars in the creation of a typology of self-exclusion mechanisms.

This study explains why horizontally connected self-exclusion mechanisms are more reliable than disconnected mechanisms when it comes to protecting gamblers. In general, connected mechanisms enable data exchange among service providers who are included in them. For this reason, such systems provide a greater guarantee that self-excluded online gamblers will not be able to gamble during their self-exclusion periods. Due to the non-harmonized nature of national legislations, however, the rules of data exchange have not been stipulated, and hence the protection of gamblers may be undermined.

Horizontally disconnected but vertically regulated self-exclusion mechanisms are also effective in identifying self-excluded online gamblers, at least in particular jurisdictions (national, international or supranational). Whereas in horizontally connected systems service providers must harmonize their identification mechanisms (a difficult task due to the fragmented legislative landscape in Europe), with horizontally disconnected (but vertically regulated) mechanisms the situation is considerably different.
Service providers included in horizontally disconnected and vertically regulated mechanisms must develop an identification infrastructure to be capable of effectively exchanging data with only one entity— that which manages the central database of self-excluded online gamblers.

Horizontal (dis)connectivity depends on applied regulations, and hence regulatory arrangements shape the second dimension of the typology of self-exclusion mechanisms. Self-regulated mechanisms (those that are vertically unregulated) can ensure data exchange by creating interoperable databases of self-excluded online gamblers. These mechanisms can overcome the regulatory obstacles that affect vertically regulated systems. However, ensuring the lawfulness of the processing of online gamblers’ personal data in vertically unregulated mechanisms is more difficult than in vertically regulated mechanisms. Whereas in vertically regulated systems compliance with mandatory legislation, data subject consent and legitimate interests can serve as grounds for the lawfulness of data processing, in unregulated systems data subject consent seems to be the only acceptable ground. Nevertheless, even consent is problematic in this regard due to the requirement of informed and freely given consent, which is difficult to meet in the online ecosystem in general in the context of self-exclusion in particular.

Resting the lawfulness of data processing on the ground of legitimate interests seems reasonable. Use of this ground should be approached differently in regulated (as opposed to unregulated) mechanisms, however. Online gambling service providers in vertically regulated mechanisms must comply with legislative standards adopted at the national, international or supranational level. Having the authority of the state or an international or supranational organization as a guarantee in the implementation of gambling legislation promotes legal certainty. This backing makes it easier to carry out the balancing test of estimating whether data controllers’ interests override data subjects’ rights and freedoms. In other words, it is reasonable to expect that legislation will serve as a guide for determining whether and when processing data for certain purposes is legitimate.

The dark side of vertically unregulated mechanisms lies in the fact that they can involve unlicensed service providers whose approach to the implementation of responsible gambling measures may be questionable. This raises doubts about the misuse of available data for purposes that have not been agreed to or that are incompatible with those originally stated. Therefore, demonstrating that the legitimate interests of the data controller (or third party) in an unregulated system do not override the data subject’s rights and freedoms is more difficult and uncertain than it is within regulated mechanisms.
In the end, many questions remain open in this regard. The further development of data protection regulation should bring some clarity to the matter. In the future, however, we are likely to have to deal with new emerging technologies for the promotion of responsible gambling – technologies that are likely to challenge regulators and public policymakers. Indeed, it is questionable whether conventional approaches to regulation will be preferable to approaches based on self-regulation (or other regulatory approaches). No matter what the future holds, however, what is needed is further research into the ethical, policy-related and regulatory aspects of the growing intertwinment of data processing and responsible gambling.
Bibliography


Article 29 Working Party Guidelines on transparency under Regulation 2016/679, 17/EN WP260 rev.01


Calvert v. William Hill Credit Ltd [2008] EWCA Civ 1427


International Association of Privacy Professionals, ‘Categories of Personal Information’  

International Association of Privacy Professionals, ‘ResourceCenter’  
https://iapp.org/resources/article/accuracy/ accessed 15 July 2019

International Organization for Standardization, ‘All about ISO’  
https://www.iso.org/about-us.html accessed 16 July 2019


Littler A, Member States versus the European Union: The Regulation of Gambling (Martinus Nijhoff Publishers 2011)


Pavlovic D, ‘Online gambling in the EU: from data protection to gambler protection’ (Doctoral thesis, Tilburg University 2018)

https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf accessed 16 July 2019

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) [2016] OJL119/1


Spillemyndigheden, ‘Rofus’  


