WHITE PAPER

A starters guide to provide online gambling services in a GDPR compliant manner

DPO Consultancy
Experts in Data Privacy

JUNE 2022

Claudia Arrigoni

1. The era of online gambling

The gambling industry has changed drastically over the past two decades since the rise of online gambling. The first online gambling venue was the Liechtenstein International lottery in 1994. In 2020 the market of online gambling was estimated to be worth around 66 billion dollars globally, of which Europe comprises 54%[1]. Since the start of the pandemic, the number has risen, as consumers turned more towards online platforms: the worth of the global industry is estimated to rise to 92 billion dollars in 2023.

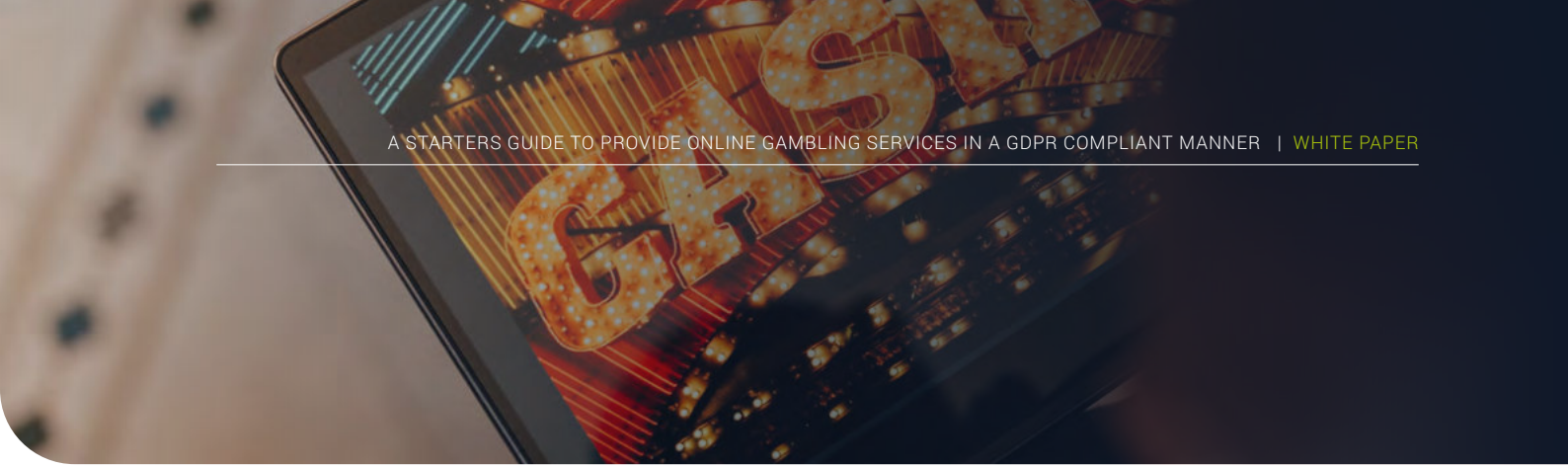
The increasing interest in online gambling among consumers offers many opportunities for international companies in the gambling industry, especially in the European market. An important factor is the increasing maturity of online gambling. Until a few years ago, online gambling was heavily restricted or even banned in some countries in the European Union, but now a change is visible. More and more countries are making online gambling available. Some countries allow all games of chance to be offered on the internet, while others only allow certain types (betting, poker, or casino games).

Challenges

Although the European market offers many opportunities for gambling companies, there are also quite a few challenges. There is no sector-specific EU legislation in the field of gambling services: EU member states are autonomous in the way they organise their online gambling services, as long as they comply with the fundamental freedoms established in EU legislation. In legal markets, online gambling service providers are required by law to have a licence to provide services and/or advertise to residents.

Not only will online gambling providers have to comply with local gambling regulations, but recent development also presents companies in the gambling industry with an even greater challenge. In online gambling, an increasing amount of personal data is being processed in a complex ecosystem. The processing of personal data is not new for many organizations, but the laws and regulations have become stricter in recent years. Especially for companies that process European personal data. Whenever organizations process personal data of

1 https://www.edisongroup.com/wp-content/uploads/2019/07/GamingSectorReport2019.pdf



individuals located in the European Economic Area (EEA), the General Data Protection Regulation (hereinafter: GDPR) applies. This remains true even if organizations are not established in the EEA: the GDPR is extraterritorial, and its rules carry across the European borders. The GDPR is a legal framework that sets specific rules, principles, and guidelines when you collect and process personal data.

Many companies in the gambling industry struggle to determine what they can and cannot do within the boundaries of the GDPR. Gambling is heavily regulated and with varying degrees of authorities monitoring every move, companies in the gambling industry are more likely to be caught tripping over regulations such as the GDPR. Additionally, the authorities monitoring privacy in European Member States (Supervisory Authorities) have varying levels of strictness.

Companies in the gambling industry want to ensure that the personal data of their users is handled with care. They want to exclude risks at an early stage, in order to avoid problems with personal data afterwards. The question is therefore how providers of gambling services can approach data processing in such a way that they can simply work safer and smarter or can gain a competitive advantage.

Guideline for GDPR in online gambling

This white paper aims to provide you with the critical activities to achieve your goals. We will explain the basic principles of the GDPR and which aspects of the GDPR you should especially consider when it comes to online gambling.

In addition, you will read how you can assess the privacy risks of your activities, so that you can take the necessary measures to reduce or eliminate these risks.

And we will show you which specific rules you should take into account as an online gambling company, in addition to the requirements of the GDPR to improve data portability, transparency and the prevention and/or reduction of personal data breaches.

2. Decide what personal data is essential for your purpose

As an organization, it is important that you know what kind of personal data you need and for what purpose. That is the basis of any processing of personal data. This should be a standard activity that any gambling service provider should perform when providing online gambling services within the European Economic Area. This way you are aware of any restrictions when processing personal data.

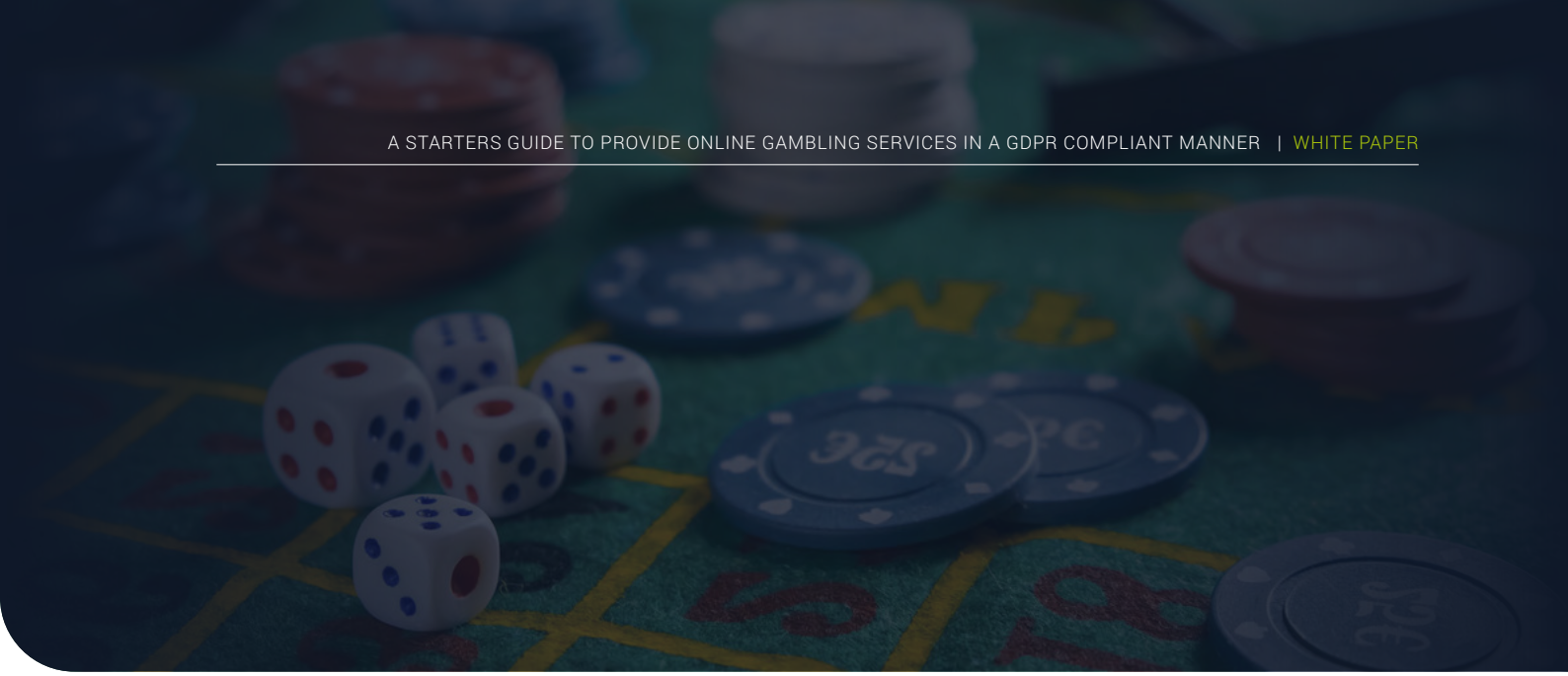
Categories of personal data

To achieve this, it is important that you are familiar with the basic elements of the GDPR. Therefore, it is useful to know what types of personal data there are. The definition of personal data is that it can be any information relating, directly or indirectly, to an individual.
The GDPR makes a distinction between 'regular' personal data[2] and 'special categories' of personal data[3]. Examples of ordinary personal data are names, addresses, telephone numbers, and email and IP addresses. The special category of personal data consists of the following:

- Either processing of data revealing:
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Trade union membership.
- Or the processing of:
  - Genetic data
  - Biometric data for the purpose of uniquely identifying a natural person
  - Data concerning health, or
  - Data concerning a natural person's sex life or sexual orientation.[4]

The above-described data is considered more sensitive in nature and therefore requires a higher level of protection. In principle, it is prohibited to process this personal data category, unless you can rely on one of the exceptions given in the GDPR or the national implementation law of the GDPR.[5] As a company in the gambling industry, for example, you are involved in legislation to combat gambling addiction. This may

2 Article 4(1) GDPR.
3 Article 9(1) GDPR
4 Article 9(1) GDPR.
5 An example is the Dutch implementation law of the GDPR: the Uitvoeringswet Algemene Verordening Gegegevensbescherming (UAVG).

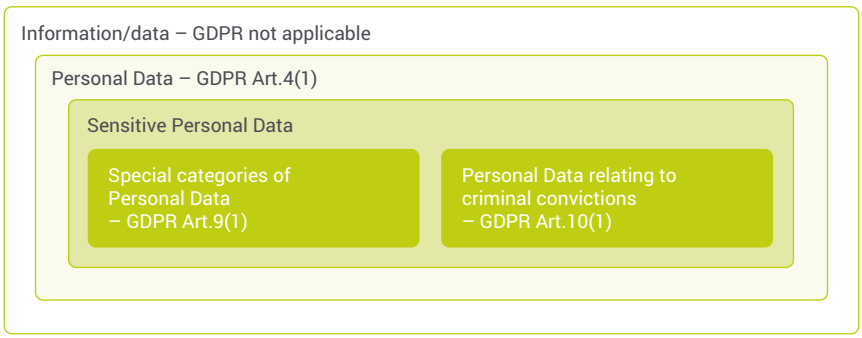


require the processing of special categories of personal data, such as a registration of people who have been banned from gambling due to problem gambling, or a Fastlane based on fingerprint scans.

Furthermore, the GDPR explains that the processing of personal data relating to criminal convictions and offenses is only allowed under the control of an official authority, or when the processing is authorized by Union or Member State law. The sensitive nature of this data requires that there should be appropriate safeguards provided for the rights and freedoms of individuals.[6]

Sensitive personal data

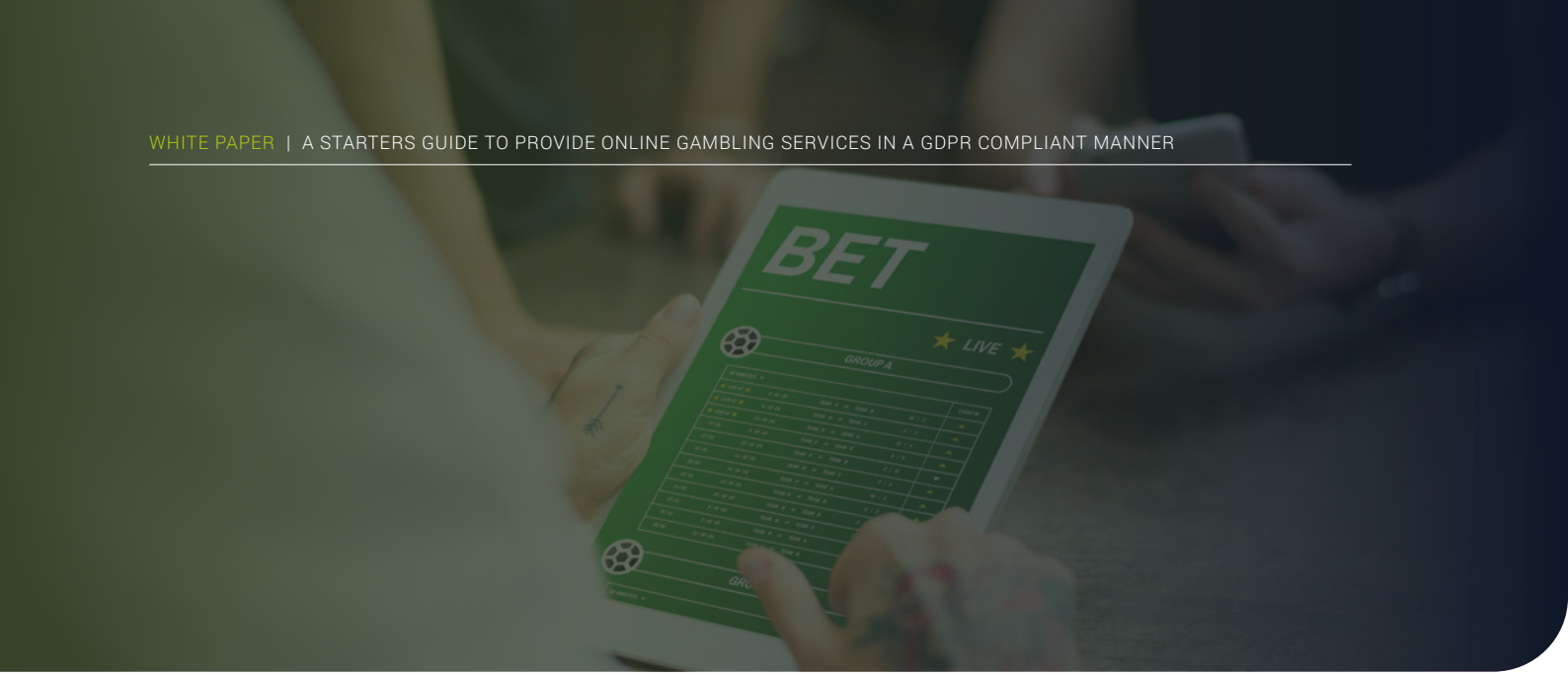
Between the regular and special categories is an unofficial category called 'sensitive'. This is personal data that is not included in the definition of special but is too sensitive to be treated as ordinary personal data and therefore deserves more protection. Examples of sensitive personal data are financial personal data or credit card data.



National identification numbers

The GDPR also explains that Member States may further determine conditions for processing national identification numbers. Therefore, you need to be cautious whenever national identification numbers are processed.[7]

6 Article 10 GDPR.
7 Article 87 GDPR.



Regular personal data

The 'regular' personal data, consist of all the data that falls outside of the categories described above. It is, however, recommended to always think logically and assess the sensitivity of personal data to implement the appropriate technical and organizational measures to protect the data. You can imagine that a name is far less sensitive than an individual's financial data, such as a bank account number.

Processing

The next step is to understand what 'processing of personal data' means? Processing is **any** operation that is performed on personal data, such as:

- Collecting
- Recording
- Organising
- Structuring
- Storing
- Adapting
- Altering
- Retrieving
- Erasing
- Disclosing
- Disseminating (making available)
- Consulting (reading)
- Aligning or combining
- Restricting
- Destroying

These definitions by the GDPR are not exhaustive. It is impossible to imagine an activity that is not regarded as processing. So as soon as you are dealing with personal data, you are processing it.

Key Players

It is also important to understand that the GDPR distinguishes between three types of players that play a key role in the processing of personal data: the controller, the processor(s), and the data subject(s).

Controller	Organization	The party that, alone or jointly with others, determines the purposes and means of the processing of personal data
Processor(s)	Partners, contractors	The party that processes personal data on behalf of the controller
Data subject(s)	Organisation's employees, customers	The identified or identifiable natural person

The relationship between a controller and a processor is important and the respective responsibilities are decided by law. It is also obligated by law to have a contract between controllers and processors (see chapter 3).

GDPR principles

Eventually, every processing of personal data should lead back to the principles of the GDPR. Article 5 of the GDPR lists seven principles. To understand GDPR compliance in data processing activities, it is crucial to know each of them as it affects every data processing operation. These are the principles:

1 The principle of lawfulness, fairness, and transparency

Every data processing should be valid under the GDPR and should not breach any other relevant laws. Furthermore, the data controller should use the personal data in a way that is fair, open, and honest about how the personal data is used.[8]

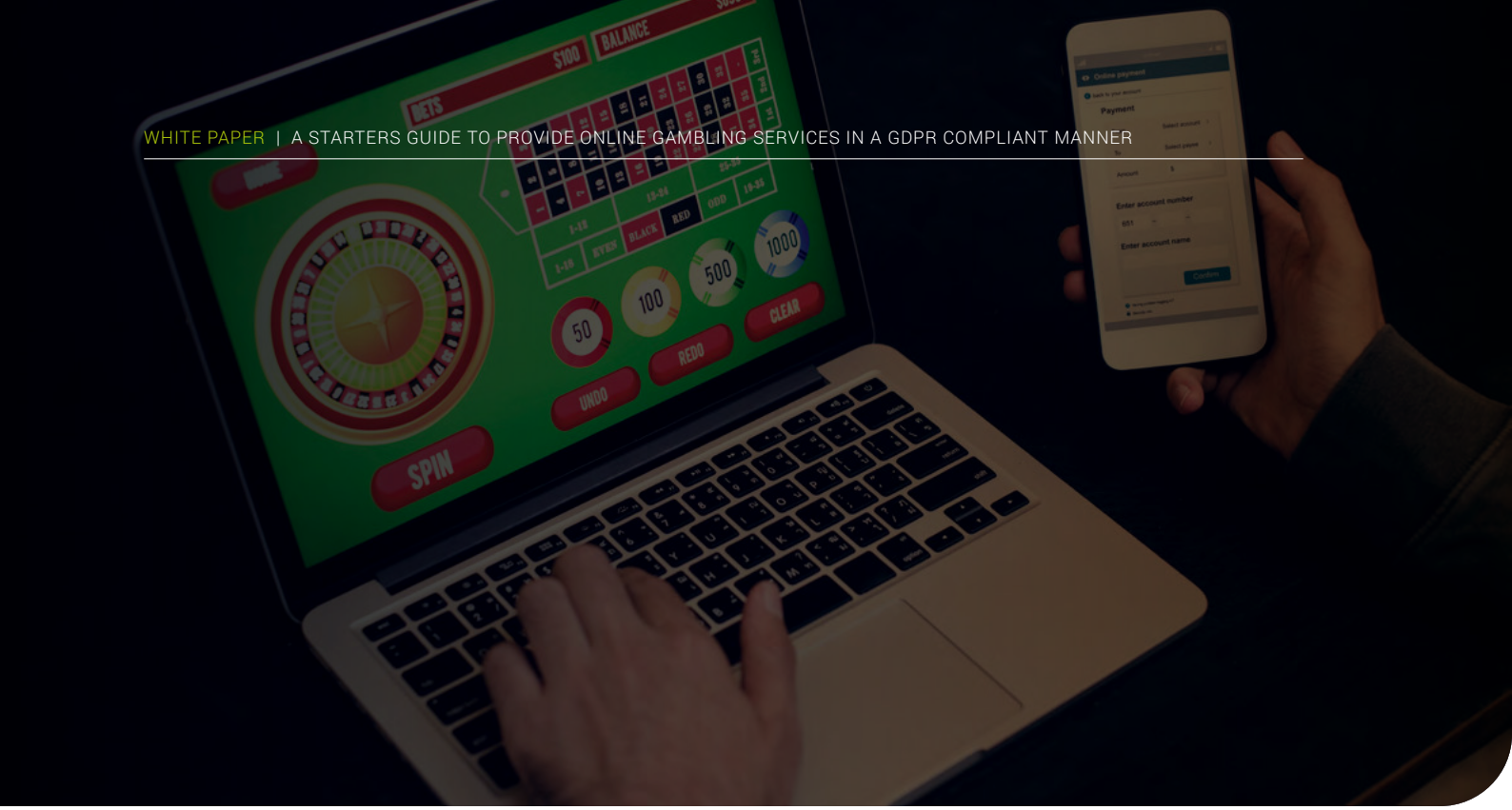
2 The principle of purpose limitation

A data controller should limit every data processing activity to a specific purpose, such as entertainment, or information services. This purpose should be specified, explicit and legitimate. The purposes need to be recorded, according to the documentation obligations under the GDPR. It also should be explained in the privacy information you provide to individuals, such as the privacy policy on the website.[9]

3 The principle of data minimization

The personal data that you process should be sufficient to properly fulfil your purpose (adequate), should have a rational link to that purpose (relevant), and you should never hold more data than you need for your particular purpose (limited to what is necessary).[10]

8 Article 5(1)(a) GDPR.
9 Article 5(1)(b) GDPR.
10 Article 5(1)(c) GDPR.



4 The principle of accuracy

A data controller should take all the necessary steps to ensure the data is correct by updating the data whenever needed. Reasonable steps should also be provided whenever personal data should be corrected.[11]

5 The principle of storage limitation

Data should never be kept longer than necessary depending on the specific purposes why the data is processed. That is why you should frequently review the stored data and should introduce a data retention policy to comply with documentation requirements. There are, however, exceptional grounds applicable whenever you need to keep data longer for public interest archiving, scientific or historical research, or statistical purposes.[12]

6 The principle of integrity and confidentiality

A data controller should ensure that there are appropriate technical and organizational measures in place to protect the data that is held against unauthorized or unlawful processing, accidental loss, destruction, or damage.[13]

7 The principle of accountability

This principle requires that you take responsibility for what is done with personal data and requires that compliance can be demonstrated with the principles described above.[14]

11 Article 5(1)(d) GDPR.
12 Article 5(1)(e) GDPR.
13 Article 5(1)(f) GDPR.
14 Article 5(2) GDPR.

Lawful grounds

Based on the lawfulness principle, lawfully processing personal data requires a legal basis provided by the GDPR. If there is no legal basis, no personal data may be processed:

1. **Consent:** such as the well-known opt-in for sending marketing emails,
2. **Contract:** such as the employment contract on the basis of which personnel data must be processed,
3. **Legal Obligation:** such as tax legislation that obliges to store certain personal data
4. **Vital interest:** such as processing of medical data in an emergency, - this pertains mostly life or death situations
5. **Public interest:** this only applies only to public authorities, and
6. **Legitimate (business) interest:** this only applies in exceptional cases when the business interest outweighs the privacy interest after this has been substantiated by a detailed interests assessment, such as preventing fraud.

Most organisations have a healthy mix of consent, contract, legal obligation and legitimate interest. Due to the heavy regulations on the gambling industry, legal obligations are going to be more heavy and more prominent than in other industries. Similarly, consent and legitimate interest are also going to be more relied on than usual: think of voluntary exclusion from gambling (whitelisting) or the prevention of fraud with the use of cameras.

NOTE! These lawful grounds relate to the 'regular' and 'sensitive' type of personal data. If your organisation is processing "special categories" of personal data, having a lawful ground is not enough: an exception provided by the GDPR[15] is also required.

15 Article 9 GDPR.

3. Important aspects of the GDPR for companies in the gambling industry

All businesses either established or doing business in the EEA need to comply with the GDPR. Organizations offering or aiming to offer online gambling services within the EEA will also need to comply, but there are at least three aspects that are especially important for companies in the gambling industry to attend to.

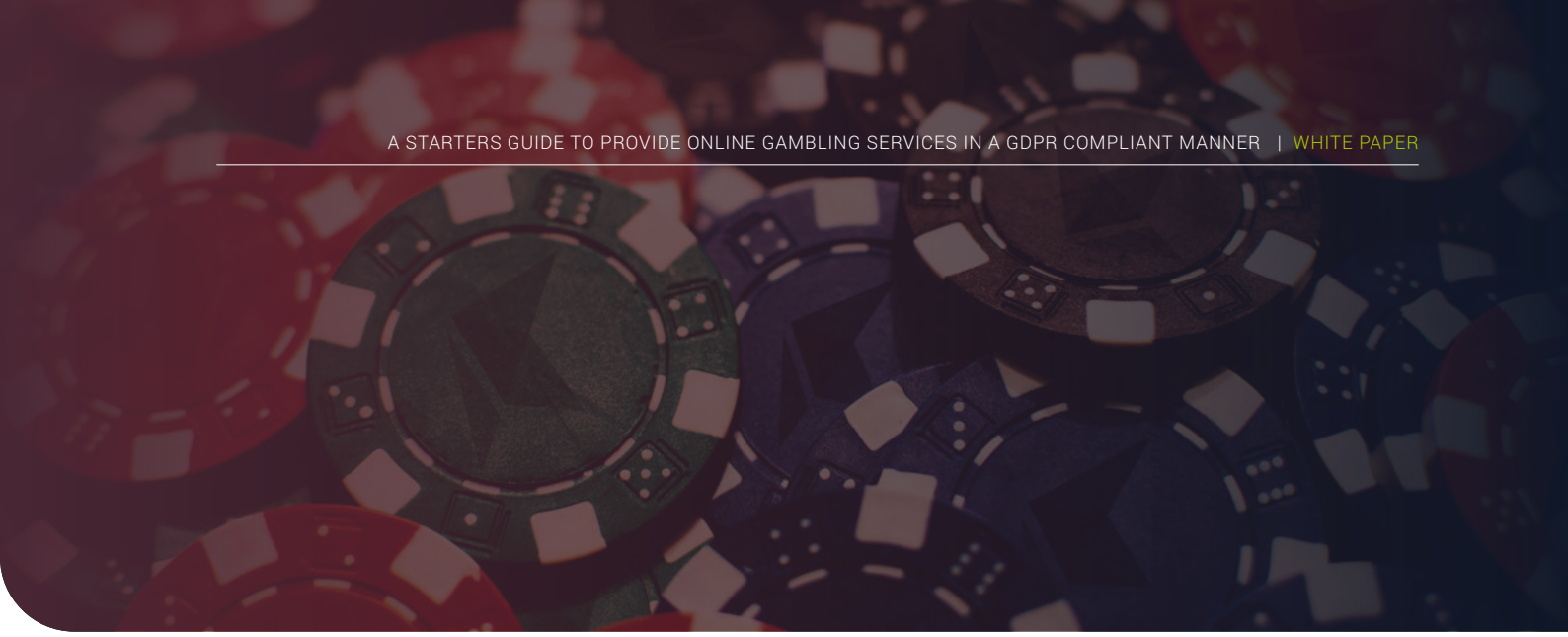
Data Processing Agreements: Partners and Contracts

Many companies that provide online gambling services operate internationally. This often means that they exchange data between their own offices in different countries. In addition, many gambling organizations also use cloud services where data from players around the world may be stored on servers elsewhere in the world.

When personal data leaves the EU for so-called third countries (think of Switzerland, United States, India, or China), the protection of the GDPR travels with the data. When this happens, it is called a data transfer: that includes making a database available for another company in another country. The rules of the GDPR therefore still apply regardless of where the data travels through or ends up in. Data transfers are not permitted in principle, but the GDPR makes an exception when using 'transfer mechanisms'. There are 4 possible transfer mechanisms, but the ones most useful and easy to apply for companies are these two:

1. **Adequacy Decision:** The country outside of the EU in question has privacy laws in place that have been deemed to provide an 'adequate level of protection' by the European Commission. The updated list of countries currently deemed as adequate can be found on their website.[16]
2. **Standard Contractual Clauses** (SCCs) in combination with a Transfer Impact Assessment (TIA). This is the most widely used transfer mechanism: it involves 4 standard contracts that cannot be amended, which simplifies the contracting process a bit. However, the biggest drawback that comes with using SCCs is that they entail a Transfer

16 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en



Impact Assessment. A TIA's purpose is to identify the risks that the transfer can have for data subjects and what measures are taken to mitigate these risks.

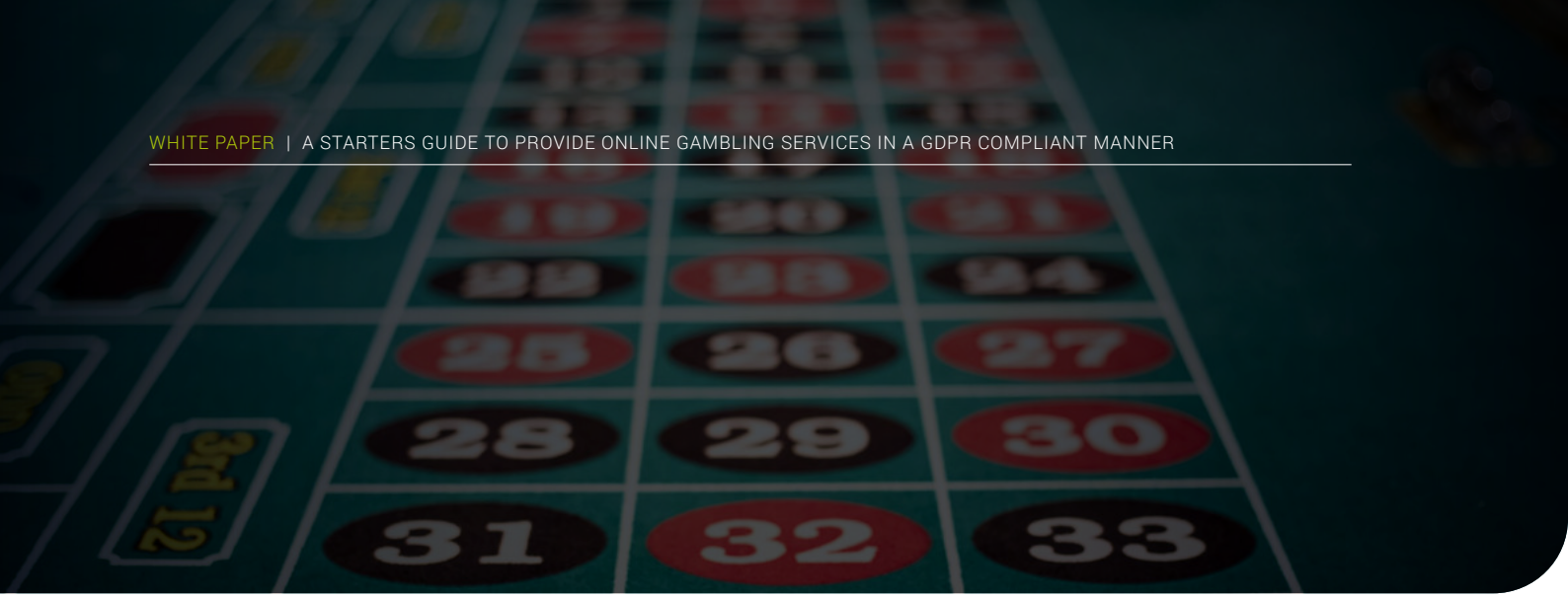
Which contracts do you need?

It is important, especially in these times when a lot of personal data is sent to, for example, the United States where there is no adequate protection for the privacy of individuals, to choose your partners carefully and to protect your players well.

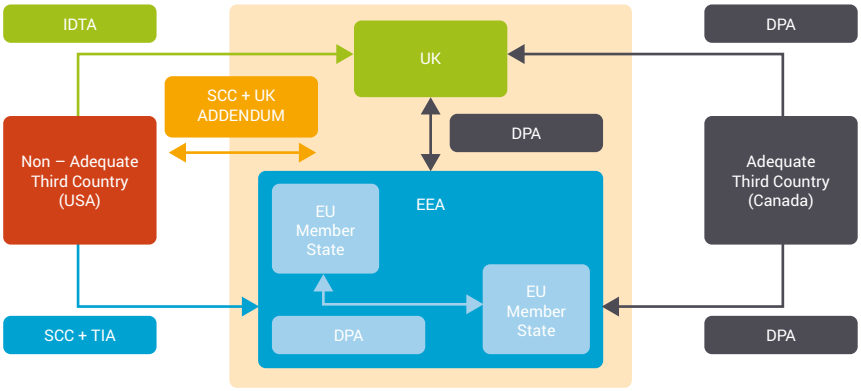
Especially if you are a gambling organization located outside the EEA or if you have partners outside the EEA, it is imperative to have contracts where the exchange of personal information is addressed. If all parties involved are within the EEA, then a simple Data Processing Agreement will be enough. If there are parties involved outside the EEA, or the UK, or both, then the situation will be more complicated.

The UK leaving the European Union has had far-reaching consequences, one of which is the UK's privacy framework. Because the UK had implemented the GDPR in 2018, but then split from the European Union, there is now the UK GDPR, a privacy legislation very similar, but at the same time completely separate from the GDPR. This has led to the UK creating their own transfer mechanisms to comply with the UK GDPR. That includes adequacy decisions, which for example have been made between the UK and the EU from both sides. This mutual adequacy decision makes it possible to freely transfer personal data between the two again.

The other common transfer mechanism that the UK uses, is a mirror to what the EU GDPR calls Standard Contractual Clauses. The UK GDPR version of SCCs are International Data Transfer Agreements (IDTAs), which will be needed when personal data is transferred from the UK to a country that is not adequate according to the UK.



Things get even more complicated when both the UK and the EU are involved with a party neither considers adequate, such as the United States of America. In this situation, then the only way to satisfy both privacy laws is with a combination of sorts, namely by concluding Standard Contractual Clauses with a so-called UK Addendum attached. That way, both the GDPR and the UK GDPR can be covered.



Data Breaches

Confidentiality and discretion are an important common good in gambling. Losing personal data is therefore an undesirable situation for every organization in the industry, as it puts pressure on the trust of consumers and suppliers. A data breach is a situation where personal data is lost, destroyed, or changed without the intention of an organization, or if unauthorized persons gain access to personal data. Examples of data breaches are:

- A stolen work laptop, tablet, or mobile phone without encryption
- A break-in by a hacker
- Sending an e-mail in which the e-mail addresses of all recipients are visible to all other recipients
- Providing personal data to an unauthorized person outside the organization

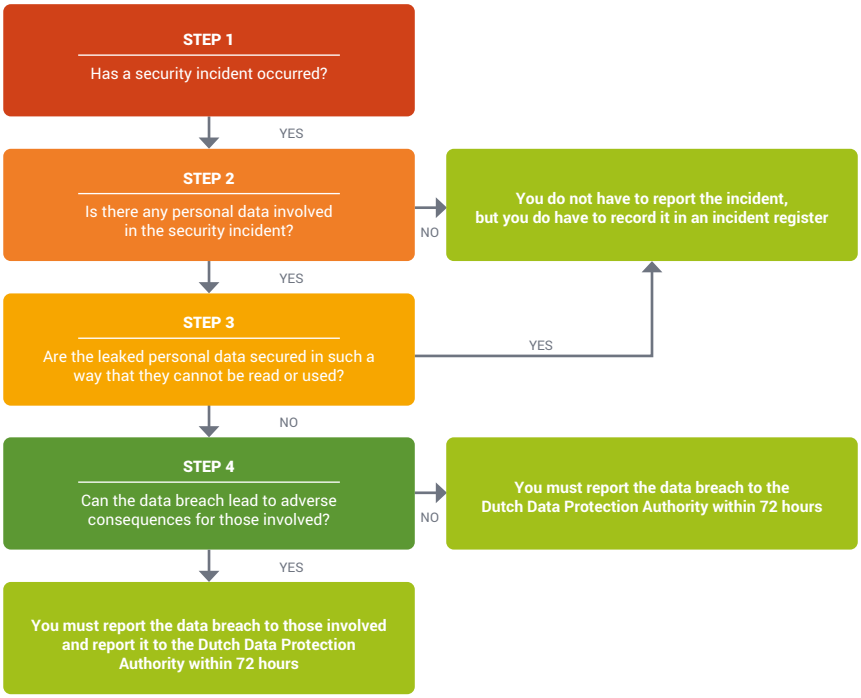
- A vulnerability in an application that allows personal data to be seen by all users
- Servers have been damaged (fire, flood, hammer) and the personal data has been lost

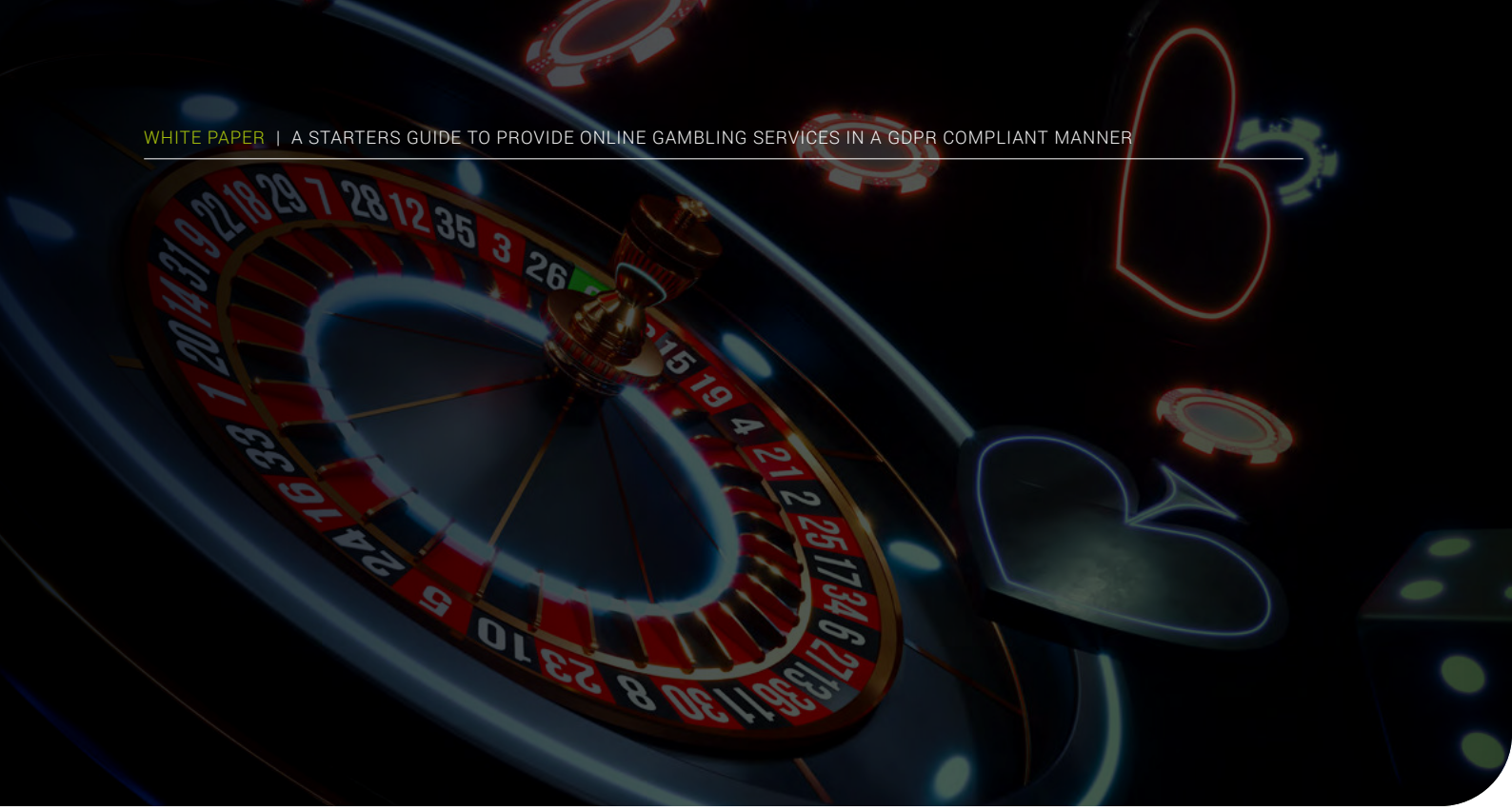
Problems usually arise when companies are hit by a serious data breach, and they are not prepared to deal with it. After trying to mitigate damage, reinstalling backup data, and after the initial panic has subsided, companies usually remember (if they know it at all) to report the data breach. That's usually when they find out there was a very strict deadline of 72 hours for reporting a data breach after becoming aware of it. A deadline that they didn't meet, and now they're being fined for reporting the data breach too late.

Data breach protocol

To avoid this situation, it is important to know how to identify a data breach, to assess its severity and potential damages, and especially when to report a breach. Data breaches of a certain severity need to be reported to the relevant supervisory authorities, and sometimes a notification needs to be made to the affected individuals. The steps that your organization needs to take are described in a data breach protocol. The purpose of a data breach protocol is to deal with the consequences of a data breach in a controlled manner. It is a plan with which organizations can determine whether a data breach should be reported, how this should be done and who plays which role if there is a data breach. The flowchart below lists the various questions that your organization must answer in the event of a data breach.

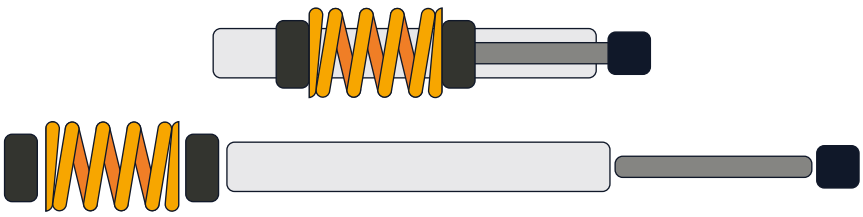
Want to know more about how to draw up a data breach protocol for your organization? Check out our tool for a step-by-step data breach protocol.





Data Protection Impact Assessment: disassemble the process and identify risks

It is very likely that your organization has to carry out a Data Protection Impact Assessment (DPIA). This is a process designed to help your company systematically analyze, identify and minimize the privacy risks of a project or plan. Essentially, what a DPIA does is disassemble the process to its smallest components and assists in identifying possible risks. A DPIA does not have to make all risks disappear but helps to minimize and determine whether the level of risk is acceptable in the circumstances.



A DPIA is similar to disassembling a tool. The goal is to find possible risks by looking at all small components

Performing a DPIA is required when a company initiates a new or changed processing of personal data that is likely to impose a “high privacy risk” on the individuals involved. Sometimes, depending on the processing, a DPIA can even be required by the local supervisory authority, as in the Netherlands when installing security cameras, or using biometric data such as fingerprints or facial recognition.

9 criteria for when to perform a DPIA

There is no clear definition of when you should perform a DPIA, but, for example, the European Data Protection Board has drawn up 9 criteria. If you meet one of these criteria, the European Data Protection Board (hereinafter: EDPB)[17] states that you will most likely need to perform a DPIA.

1. Assessing people based on personal characteristics

This includes profiling and forecasting, based on characteristics such as a person's professional performance, economic situation, health, personal preferences or interests, reliability or behavior, location or movements.

2. Automated decisions

This concerns decisions that have legal or comparable substantial consequences for the data subject. Such data processing can, for example, lead to people being excluded or discriminated. Data processing with little or no impact on people does not fall under this criterion.

3. Systematic and large-scale monitoring

This concerns monitoring of publicly accessible areas, for example with camera surveillance. Personal data can be collected without the data subjects knowing who collects their data and what happens to it afterwards. In addition, it may be impossible for people to avoid this data processing in public places.

4. Sensitive data

This concerns special categories of personal data (see chapter 2), such as information about a person's political preferences. This also includes criminal data and data that is generally regarded as privacy-sensitive, such as data about electronic communication, location data and financial data.

5. Large-scale data processing

The GDPR does not define 'large-scale data processing'. The European privacy supervisors advise to determine whether this is the case with the following criteria:

- the amount of people whose data is processed;
- the amount of data and/or the variety of data being processed;
- the duration of the data processing;
- the geographical scope of the data processing.

6. Linked Databases

This concerns data collections that are linked or combined with each other. For example, databases that arise from two or more different

17 The European Data Protection Board (EDPB) is an independent European body, established by the GDPR. The EDPB contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities.

data processing operations with different purposes and/or carried out by different controllers, in a way that data subjects cannot reasonably expect.

7. Data on vulnerable persons

When processing this type of data, a DPIA may be necessary because there is an unequal power relationship between the data subject and the controller. As a result, data subjects cannot freely give or refuse permission for the processing of their data. This may concern, for example, employees, children, and patients.

8. Use of new technologies

The GDPR is clear that a DPIA may be required when using new technology. This is because this use may involve new ways of collecting and using data, which may pose significant privacy risks. The personal and social consequences of using a new technology may even be unknown. A DPIA then helps you to understand and remedy the risks.

9. Blocking of any right, service, or contract

This concerns data processing that results in data subjects:

- not be able to exercise a right or;
- not be able to use a service or;
- unable to conclude a contract.

For example, a bank that processes personal data to determine whether they want to provide a loan to someone.

What should be assessed in a DPIA for online gambling?

A DPIA is form-free, but there are multiple elements to assess to identify potential privacy risks for the individuals involved. It is a great tool to put a processing activity under a magnifying glass, so that the entire data journey from input to output is assessed. And additionally, to assess whether all obliged conditions are in place.

Elements that can be assessed are, for example, which individuals are involved (e.g. the 'vulnerable' like the elderly, people with a gambling problem, etcetera), what type of data is processed (e.g. health data, financial data, biometric data, location data), whether the data is appropriately secured, and which external parties are involved (and if all the GDPR requirements have been met with regard to, for example, data processing agreements), etcetera.

4. Specific rules for online gambling companies

In 2020, the EDPB published a draft Code of Conduct (The Code) on data protection in online gambling[18]. The code goes beyond the requirements of the GDPR and introduces specific rules for online gambling companies aimed, for example, at improving data portability, transparency and preventing and/or mitigating personal data breaches. The code is expected to be formally adopted and implemented by all other national data protection authorities in the EU in 2022.

The Code addresses specifics of the online gambling industry, providing businesses with clarity on areas where interpretation of the GDPR implementation is needed. For example, regarding the use of personal data to problem gambling. This way, you can ensure your customers are reassured that their personal information is being used appropriately. The Code establishes several important obligations of companies in the gambling industry that process personal data within the EU:

- You must be able to identify and understand the personal data that you are processing;
- you must ensure that you comply with the legal obligations regarding the processing of that personal data; and
- you must be able to account for and document compliance activities.

To deliver upon these obligations you must establish a compliance framework. A compliance framework should cover the following core activities:

Data mapping

You are expected to perform a data mapping exercise that results in the creation of data maps (over one or more documents). There is no specific template for a data map and it can take various forms. Think of diagrams, spreadsheets, databases or templates using privacy management software. Proper data mapping will need to go further than the minimum requirements for 'records of processing', which is a high-level summary of personal data use required of all organizations.[19] You are expected to have investigated and mapped your use of player

18 https://www.egba.eu/uploads/2020/06/200211-Code-of-Conduct-on-Data-Protection.pdf

19 Article 30 GDPR.

personal data. Process of conducting data maps and their structure depend very much on the structure of your organization, technical infrastructure and how your organization processes personal data (operational procedures).

The EDPB has listed some of the best practice requirements for data mapping:

1. Where feasible, data mapping should cover:
   - what personal data is processed (whether created, collected or acquired);
   - the source of the personal data;
   - how personal data enters and leaves the organization (including who the recipients of personal data may be) and its flows within the organization;
   - the location of the personal data (not just the geographic location but the system(s) on which it is held); and
   - what the personal data is used for.

2. Your data mapping should record personal data at a 'field level'. So, the recording of a player's postal address should be stored line by line, rather than as one continuous block of text. You register each line as a separate field.

3. You must record every occurrence of any personal data. For example, a player's email address is likely to reside in multiple databases, spreadsheets, and relevant physical documents. That means you must register each location, as it relates to a separate processing activity.

4. Personal data that is encoded or held in encrypted files should also be included.

5. It should be possible to know the location (geographic/site and system based) of any piece of personal data easily from any resulting data maps within 24 hours.

6. Perform a lifecycle analysis of player data to understand how it is processed, from creation/collection, through corporate use, to eventual deletion. This is often captured by means of a 'process flow map' (usually in diagram form) to capture the flows of personal data to and from the operator, paying particular attention to where personal data has been added or enriched during this process.

Lawful Processing Analysis

Once you have collected the information about your processing activities through data mapping, you can conduct an analysis of the lawfulness of your processing[20]. This means that for each processing activity, the legal basis on which you rely must be considered. This analysis is essential to ensure adherence to the key principles of fairness, lawfulness, and transparency. Without the lawful basic analysis and data mapping, you are not able to write a compliant privacy policy or determine when it was appropriate to update the privacy policy, due to changes in processing. This analysis also helps you to ensure that any personal data located, and any processing identified, meets the other GDPR principles.

Risk Assessment

You will have to review the results of the data mapping to determine other risks and consequent actions that may exist in terms of data protection compliance. You can use the data maps to determine the extent to which personal data is currently being processed in the company that is not needed or is disproportionate. This will be key for compliance with the purpose, data minimization, storage limitation and integrity and confidentiality purposes.

The risk should be evaluated depending on the processing activities and the areas that are assessed. Any risk assessment can be used as long as it's documented and repeatable. If you discover that personal data is stored in an unnecessary or inappropriate location, that data should be reviewed and securely destroyed or moved. A root cause analysis should be performed to understand if a policy or process review is needed to prevent recurrence. This is the first step in a continuous improvement cycle.

20 Article 6 GDPR

Documentation

Accountability is a core principle of the GDPR (see chapter 2 of this paper). That is why the EPDB requires that you have certain core documentation to demonstrate that you comply with the principles and requirements of the Code. The following documents are the minimum required to create a compliance framework:

- the data maps that you created.
- a record of processing activities, being the GDPR required document that your supervising authority will expect to see.
- a policy including governance of processing activities and the reviewing and maintaining of the data map and record of processing activities.
- a policy which includes the involvement of the DPO, in all work affecting the processing or flow of personal data – privacy by design, methodology or any other procedure that explains this concept and its implementation.

All documents must be version controlled and must be reviewed and authorized at least annually. Where any of these documents are used to support a business decision, the appropriate version of that document must be referred to.

Review, assessment, and amendment

Ensuring continual demonstrable compliance is crucial. You will be expected to have in place processes to ensure that the required documentation is being reviewed and kept up to date to ensure compliance with the Code and the GDPR. Periodic internal or external audit shall form a part of this review.

All such documents shall be version controlled. Evidence of compliance used as part of any audit, including those related to compliance with the Code, must be retained for a minimum period of 3 years from the end date of the activity.

8 Idem, p. 44-46.

5. Self-scan for data privacy in online gambling

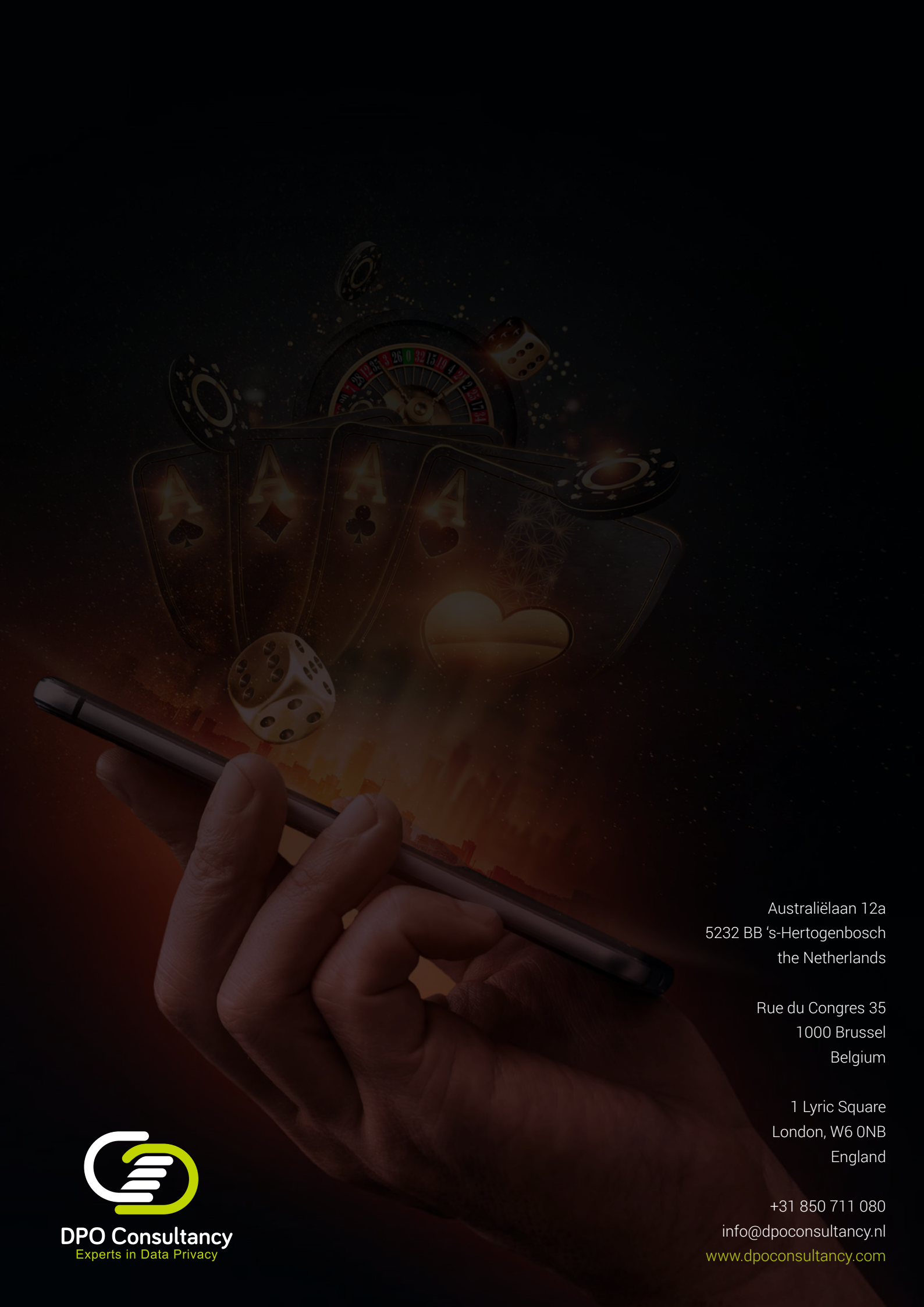
In this white paper, we have given you the tools to continue creating value with your online gambling services in a GDPR compliant manner. In summary, the content of this whitepaper boils down to the following three key topics:

- Deciding what personal data you need for your purpose
- Which important aspects of the GDPR are specifically important for companies in the gambling industry
- Which specific rules there are for online gambling companies

You are now better aware of what the GDPR entails if you are active in the online gambling industry. You also know how to process personal data in a safe and responsible manner and how to comply with the privacy rights of your users. But where do you start and how do you determine where you are now? To help you on your way, here's a quick self-scan which will help you determine how far your organization has evolved in the field of data privacy. By answering these questions, you immediately see where to improve, in which areas you already excel and where the emphasis should be for the coming period.

Question	Answer	
What is your role in the data processing?	Controller/Joint-controller/Processor	
What personal data do you process and how do you protect it? And for what purposes exactly?	Regular data:	Purpose(s):
	Special category of data:	Purpose(s):
	National identification number:	Purpose(s):
	Other sensitive data:	Purpose(s):
Do you know what a data processing agreement is and whether you have concluded one with your partners?	Yes/no (if yes, explain what data you process and with which partners)	
Do you have a Data Protection Officer?	Yes/No (Do you know what a DPO does?)	

Question	Answer
Are you aware of the rights of your customers and employees under the GDPR?	Yes/No
Are you a party, or do you have contracts with parties, outside the European Union?	Yes/No (If no, do you know how/or the privacy of your customers or employees are protected in those countries?)
Does your organization have a data breach protocol?	Yes/No (If no, does your organization know when to report a data breach and to whom?)
Do you know which of your organization's activities warrant DPIAs, and have you conducted these?	Yes/No (If no, what processing activities are not assessed?)
Is your organization's privacy notice/privacy policy up to date?	Yes/No Last update date on notice/policy:
Did your organization implement a process to manage data subject rights request?	Yes/No



DPO Consultancy
Experts in Data Privacy

Australiëlaan 12a
5232 BB 's-Hertogenbosch
the Netherlands

Rue du Congres 35
1000 Brussel
Belgium

1 Lyric Square
London, W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com