

Code of Conduct on Data Protection in Online Gambling



CONTENTS

I. About this Code	1
II. The Requirements	3
III. Case Studies	44
IV. Conditions of Adherence	49
V. Governance of the Code	53

Annex A: Template Declaration of Adherence

Annex B: List of concerned Supervisory Authorities

Annex C: List of documents for the operators' compliance framework

I. ABOUT THIS CODE

What is this Code for?

This code of conduct for online gambling operators (hereafter '**the Code**') provides guidance for operators of online gambling services in processing personal data in compliance with the General Data Protection Regulation ('**GDPR**').

The Code provides important guidance and rules in relation to the personal data processing activities through the use of case studies, summaries and examples of good practices for operators. It addresses specific features of the online gambling services sector, providing operators with clarity on areas where interpretation on GDPR implementation is needed, as well as ensuring that players feel confident that their personal data is used appropriately. The Code takes into consideration the guidelines of the European Data Protection Board ('**EDPB**'), as well as the guidelines issued by the different Supervisory Authorities ('**SAs**').

Who does this Code apply to and what is its status?

This Code is a code of conduct that has been prepared and approved pursuant to Article 40, GDPR. It applies to, and will be enforced against, its members but is also open for voluntary adherence by other online gambling operators. It is monitored by in accordance with Article 41, GDPR as set out in more detail in section V of this Code.

What does the Code cover?

It covers the data processing of players' personal data. The Code does not cover processing of personal data in the context of: (i) the company-employee relationship; or (ii) offline activities, for example, in bricks and mortar betting or gambling establishments.

How does the Code accommodate changes and local law requirements?

The Code is drafted to be fully consistent with the GDPR at the time of writing. The Code is, however, to be read as a living document, intended to be further developed over time, as practical issues arise with the effective implementation of the GDPR and in view of further EDPB guidelines.

In the event of any changes in EU data protection law, or to any law that would impact the content of the Code, a member is required to comply with the new legislation, even if such legislation has not been implemented yet in the Code, and even if this would entail new or conflicting obligations regarding the Code.

The Code is based on the GDPR and does not cover the local derogations that exist at a Member State level which members are responsible for ensuring compliance with. Declaration of adherence to the Code does not absolve a member from having to comply with other applicable EU or Member State data protection law. In any case in which a Member State has stricter or different rules regarding data protection than those set out in this Code, such national provisions shall take prevalence. A member shall not lose membership of the Code or enforcement under it in the event of such a conflict, provided that the member has documented the contradictory requirements and why an alternative approach should be taken.

Adherence to the Code should not result in any operator having a conflict between the Code and its internal policies, procedures or standards. Any such conflict must be resolved before declaring adherence to the Code.

How do we use this Code?

Part II of the Code contains the relevant requirements for members. Section II.2 of that Part focuses on the initial establishment of a compliance programme to enable compliance with the Code and the detailed requirements which follow in sections II.3-9 of Part II.

Part 0 of the Code assists members in providing some specific case studies as to how to apply the requirements to certain common personal data processing scenarios that members may face.

Parts 0 and V provide details of the conditions for adherence to the Code (i.e. how to become a member) and how the Code will be governed, monitored and enforced.

II. THE REQUIREMENTS

1. OVERVIEW

This Part II summarises the key obligations on operators under the GDPR and how they should be interpreted. The overriding obligations of an operator are to:

- identify and understand the personal data which it processes;
- ensure that it understands and complies with the legal obligations on it in relation to the processing of that personal data; and
- be accountable for and document its compliance activities.

2. COMPLIANCE FRAMEWORK

In order to deliver upon the obligations set out in section 1 above, an operator must establish a compliance framework that will support adherence to the Code. This section explores what this compliance framework should comprise and cover. The remaining sections 3-9 then provide more detail on the specific articles of GDPR and requirements of the Code and how they should be met by operators under this Code.

A compliance framework should cover the following core activities which are each explained in turn in this section 2:

- Data Mapping
- Lawful Basis Analysis
- Risk Assessment
- Documentation
- Review, Assessment and Amendment

➤ **The operator shall establish a compliance framework to support the adherence to the Code.**

2.1 **Data Mapping**

Achieving compliance with the Code requires a detailed understanding of the personal data which is being processed by an operator. Without this foundational understanding, it will not be possible for an operator to comply with the GDPR or this Code including the principles of transparency, accountability, data security and data minimisation as well as the rights of access, erasure, rectification and portability.

Operators are expected to undertake a data mapping exercise resulting in the creation of data maps (across one or more documents). There is no one specific template for a data map and it may take several forms (for example, it may incorporate diagrams, spreadsheets, databases or templates using privacy management software).

It is important to note, however, that 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 operators under Article 30, GDPR. Many SAs provide templates for

such records of processing which provide a useful guide, but the data mapping outlined in this section will need to go much deeper and supplement this record.

Under this Code, operators are expected to have investigated and mapped their use of player personal data. Process of conducting data maps and their structure depend very much on the structure of the organization, technical infrastructure and how the organization processes personal data (operational procedures).

- **The operator shall develop a data map of player's data.**
- **The data map should contain the minimum requirements mentioned in the paragraph above. Below listed best practice requirements, are not mandatory but can be applied by the operators depending on their structure, organization and other factors.**

In addition, below are the best practice requirements for data mapping:

- 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 organisation (including who the recipients of personal data may be) and its flows within the organisation;
 - 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.
- It should record personal data at a 'field level'. This form of recording would, for example, involve the recording of a player's full name in two or more fields: e.g. 'forename' and 'surname'. Similarly, a postal address would be stored line by line (rather than as one continuous block of text) where each line is recorded individually as a separate field.
- It should record every occurrence of each personal data. For example, a player's email address is likely to be contained in multiple databases, spreadsheets and relevant physical documents, meaning that each location must be recorded since this relates to a separate processing activity.
- Personal data that is encoded or held in encrypted files should also be included.
- 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.
- Carry out a life-cycle analysis of player data to understand its processing from creation/collection through use within the business to eventual deletion. This is often captured through a 'process flow map', usually in diagram form, to capture personal data flows into and out of the operator, taking particular note of where personal data has been added to or enriched during this process, for example, by a data processor.

2.2 Lawful Processing Analysis

Once operators have collated the information about their processing activities through the data mapping exercise in section 2.1 above, they will be able to conduct an analysis of the extent to which their processing is lawful.

This will involve consideration of the lawful basis upon which the operator is relying for each processing activity. This analysis is essential to ensure compliance with the key principles of fairness, lawfulness and transparency explained in section 3.1 of Part II of this Code. Without the lawful basis analysis, and the data and flow mapping which it relies upon, an operator would be unable to write a compliant privacy policy with any degree of confidence or to determine when it was appropriate to update the privacy policy, due to changes in processing.

This analysis exercise also helps operators to ensure that any personal data located, and any processing identified, meets the other principles or purpose limitation threefold test and minimisation explained in sections 3.2 and 3.3 of this Part II of this Code.

The analysis of the lawful basis should document it for each processing activity; remembering that processing includes gathering, storing and destroying personal data. The method of recording this analysis can be determined by the operator.

Should any personal data processing be identified where the lawful basis is not clear, this must be flagged as a priority issue for the Data Protection Officer ('DPO').

- **The operator shall conduct an analysis on the lawful basis used for the processing of personal data.**
- **The analysis should document the lawful basis for each processing activity.**

2.3 Risk Assessment

In addition to the lawful basis of processing assessment, operators will need to review the data mapping results to determine other risks and resulting actions which may exist in terms of data protection compliance.

In particular, operators can use the data maps to determine the extent to which any personal data is currently being processed in the business, which is not in fact needed or is disproportionate. This will be key for compliance with the purpose, data minimisation, storage limitation and integrity and confidentiality purposes in particular as explained in sections 3.2 to 3.6 of Part II of this Code.

The risk will be evaluated depending from the processing activities and the areas that are assessed. Any risk assessment can be used as long as it's documented and repeatable.

For example, when conducted at a field level, the data and data flow mapping can help recognise different risk profiles associated with different personal data fields or combinations of fields, such as direct and indirect identifiers. A direct identifier, capable of identifying a player without combination with other fields such as an email address, may pose a higher risk to that individual's rights and freedoms than a single indirect identifier such as an IP address. However, multiple indirect identifiers when combined, may constitute a significant risk.

Should the data mapping exercise detect personal data stored in an unnecessary or inappropriate location, such data shall be reviewed and securely destroyed or relocated. A root cause analysis must be conducted, to understand whether a review of policy or process is necessary to prevent reoccurrence, forming the first stage in a continual improvement cycle.

- **The operator shall conduct a risk assessment to determine the level of risk posed to the players by all forms of processing, including storage and transmission.**
- **Where unacceptable risks are identified the operator shall put in place risk mitigation actions to reduce the risk to acceptable levels. The risk assessment should be reviewed on a regular basis.**
- **The risk assessment process shall be documented, consistent and repeatable.**

2.4 Documentation

Accountability is a core principle of the GDPR. The establishment of a compliance framework will therefore involve the creation of certain core documentation to demonstrate compliance with that principle and Code requirements. The following documents are the minimum documents required for creation of a compliance framework in this respect:

- the data maps created under section 2.1;
- a record of processing (if separate from the data map), being the GDPR required document that SAs 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 authorised 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.

- **As part of its compliance framework, the operator shall possess/have: i) data map(s); ii) record of processing; iii) policy including governance of processing activities; iv) policy including the process of ensuring the involvement of the DPO in all work affecting the processing or flow of personal data.**
- **All the documents of the compliance framework, must be version controlled and must be reviewed and authorised at least annually by the DPO and progress in the field will be reported to the highest levels of management to which the DPO reports.**

2.5 Review, Assessment and Amendment

Ensuring continual demonstrable compliance is crucial.

Operators will be expected to have in place processes to ensure that required documentation created as part of this section 2 are regularly 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.

- **Periodic internal or external audit shall form a part of establishing these processes.**
- **The operator shall retain for at least 3 years, from the conclusion of the audit, the evidence of compliance used as part of any audit.**

3. PRINCIPLES OF PERSONAL DATA PROCESSING

This section 3 provides clarity and further guidance for operators regarding compliance with the principles contained in Chapter II, GDPR. In particular, Article 5, GDPR specifies that the following principles of data processing must be met: lawfulness, fairness and transparency;

purpose limitation; data minimisation; accuracy; storage limitation; availability; integrity and confidentiality. Articles 6 – 10 of the Chapter then provide specific additional obligations around processing under the ‘lawfulness’ element of the first principle in particular. Each principle is considered below with practical examples for operators.

3.1 Lawfulness, Fairness and Transparency

There are three components to this principle:

3.1.1 Lawful

To ensure processing is lawful, an operator must determine, for each processing activity, which of the specified ‘lawful basis of processing’ it is relying on and ensure that it meets the requirements of that lawful basis. Operators must first consider the lawful bases set out in Article 6, GDPR. Then, if the operator is processing special category data, it must also consider whether it has a lawful basis under Article 9, and if it is processing personal data relating to criminal conviction and offences, whether it has a lawful basis under Article 10.

As noted above list of legal grounds for processing personal data should be presented in the records of processing activities. The next sections consider the likely applicable lawful bases for operators with some practical examples.

➤ **The operator shall identify and document the grounds for lawful processing of personal data for each processing activity.**

3.1.1.1 Article 6 Lawful Bases

The most likely lawful bases that an operator will be relying on when processing player personal data are:

- Consent. This is a complicated basis with a lot of elements and restrictions. This is considered in more detail in section 3.1.1.2 below.
- Processing is necessary for the performance of a contract to which the player is party, or in order to take steps at the request of the player prior to entering into a contract.

Example

Personal data which an operator requires to open a player account, fulfil verification requirements, or take bet placements would all fall within “processing necessary for the performance of a contract”.

- Processing is necessary for compliance with a legal obligation to which the operator is subject.

Example

Personal data processed by an operator in order to comply with anti-money laundering legal requirements or responsible gambling obligations will be “necessary for compliance with a legal obligation”.

- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

- Processing is necessary for the performance of a task carried out in the public interest.

Example

There may be exceptional circumstances, for example, where an operator is notified of a potential suicide or harm to a player and needs to take action to protect their life. In such instances, the operator may be able to reply and/or notify the relevant authorities on the basis that the processing is “necessary in order to protect the vital interests of the data subject” but also for the overall “public interest”.

- Processing is necessary for the purposes of the legitimate interests pursued by the operator or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the player, which require protection of personal data. As with consent above, there are specific additional requirements which apply to any operator wanting to rely on this lawful basis. This is considered in more detail in section 3.1.1.3 below.

Example

It is frequently necessary to upgrade computer systems to ensure player experience remains within acceptable levels (e.g. site response time), to increase security (e.g. update the level of encryption used), and for many other reasons. These upgrades may require processing of player data to migrate it from one system to another or to decrypt it and re-encrypt it with the new standards for example.

Processing player data for these reasons is within the legitimate interests of the operator when running their business, and also benefits the player by ensuring their experience and security are maintained. Routine system updates should also be within the reasonable expectations of all players when using such a technology driven product.

Despite the fact that there will be no reasonable way to offer the player an opt-out of the legitimate interest processing, it remains possible to use legitimate interests for these purposes.

3.1.1.2 Consent

Operators considering relying on consent as a lawful basis for processing, need to be aware that there are various limitations and conditions on this basis. The GDPR sets a high standard for consent, but the biggest change to previous legislation is what this means in practice for consent mechanisms. Each of the relevant requirements for valid consent are considered below with practical examples:

- **Consent must be freely given.** Operators must not require consent from players as a precondition for the use of the service as this invalidates the use of consent as a legal basis – especially when this is not an essential part of the service. Consent should not be regarded as freely given if the customer has no genuine choice.

However, operators may carry out practices that incentivise consent in some circumstances – for example, consenting to receive email marketing about bonus promotions. Such incentives should not **penalise** players who refuse to consent to receive marketing materials (the lack of receipt of a reward or bonus etc. shall not constitute a penalty).

Example

An operator cannot require that a player gives consent for marketing purposes as a condition of opening an account because marketing is not a requirement to provide the core service of the operator. This would not be “freely given” consent.

- **Clear affirmative action:** consent must always be given through an active motion or declaration, for example, it can be obtained by using “unticked” opt-in boxes which the player must take a positive action to tick. Inaction of any kind on behalf of the player may not be used to indicate consent.

Example

An operator’s marketing team would like to use pre-ticked boxes to obtain consent to email marketing. They will not be able to do so since, in relying on inaction rather than a positive action, this will not constitute valid consent.

In contrast a change to the terms and conditions may be enacted without requiring positive action on the part of the player where the processing is not consent based. For example inaction may be taken as acceptance of changes to processing based upon a legal obligation.

- **Clear and unambiguous:** the wording of any consent needs to be clear to the player. This involves ensuring that it is clear what consent is being given to whom and for what purpose. Operators need to avoid wording that may confuse players such as double-negatives or vague references.

Example

An operator should not rely on consent with vague references such as consenting to marketing from “our selected third parties” since this is not sufficiently clear to constitute valid consent.

- **Review:** consent must be understood as an ongoing and actively managed choice, and not simply a one-off compliance box to tick and file away. Consent must be subject to review and updated if necessary. Each operator should establish their own review policy, taking into account local law requirements which can vary.
- **Granular:** operators must not bundle consents for different things together into one consent. Consents for different processing activities need to be separated out.

Example

A tick box with consent to agree to everything set out in a privacy policy would not be appropriate. First, it is unlikely that an operator in fact wants to rely on consent to everything in that privacy policy (since they are likely to have various different lawful bases they are relying on for the activities explained in it). Second, this will not be valid because it is bundling too many different activities together.

However, operators can use a single consent for different direct marketing channels (such as SMS, email, live calls) that rely on the same legal basis and are intended for the same purpose. In that case operators will need to make it clear in the text of the consent for which specific channels customer is giving the consent.

- **Documented:** operators must keep records of consent obtained with evidence of the consent being given or withdrawn, when the consent was provided, how the consent was received or withdrawn, and what information the player was given at the time of consent collection (e.g. which version of the privacy policy or fair processing notice was presented to them at the time and, ideally, a screenshot of any consent wording).
- **Separated:** consent cannot be buried in a privacy policy or terms and conditions. It must be separately and clearly presented to the player.

Example

An operator deciding to get consent from a VIP player to use their name and photograph in a promotional campaign, cannot just rely on a reference to consent being given to this, in its privacy policy. If it intends to rely on consent for the processing, it will need to consider how a clear and active, separate consent is obtained and being brought clearly to the attention of the player.

- **Easy to withdraw:** consent must be capable of being withdrawn at any time. This is important to consider for operators in deciding whether consent is an appropriate lawful basis to rely on. Operators will need to have the ability to enable players to activate this right easily and to have operationalised this withdrawal right in its system so that, if withdrawn, the affected processing activity no longer happens. Where processing is based on consent, the withdrawal of consent will also impact personal data processed by processors or sub-processors in relation to the consent. The most common mechanisms used by operators for enabling the withdrawal of consent are (by way of example only):
 - (i) **Marketing emails:** unsubscribe links at the bottom of each marketing email.
 - (ii) **Marketing SMS messages:** texting 'STOP' to a number given in the text message. It should be clear to players whether they need to send this directly to the operator or to the SMS provider.
 - (iii) **Preference management centre:** giving players the options to sign into their accounts and withdraw their consent for each means of communication (for example to different marketing preferences) through custom settings within the account.
 - (iv) **Cookies:** cookie management software solutions that allow players to change their permissions for different types of cookie solutions via the website or app.

Operators will most commonly need to consider consent as a lawful basis in the context of cookies and other direct marketing activities where legitimate interest would not be a lawful basis. Section 0 of this Code includes a case study on direct marketing consent and the considerations to be taken into account there.

- The operator shall not require consent from players as a precondition for the use of the service.
- When it's possible to incentivise consent, the operator shall not penalize any player who refuses to consent to certain processing of personal data.
- The mechanisms for consent shall always require consent to be given through an active motion or declaration.
- The operator shall present any request for consent in a plain, easily accessible way.
- The operator shall present any request for consent separately from any other contractual clauses, privacy policy provisions or terms and conditions.
- The operator shall update and review consent when needed. The operator should establish its documented review policy for how consents are managed.
- The operator shall never bundle together consents for different processing activities and each request shall be separate and distinct.
- The operator shall implement mechanisms to allow consent to be withdrawn as easily as it was given.
- The operator shall have a consent management process, which can easily demonstrate when consents are collected, the form of the consent, and record information if consents are withdrawn.

3.1.1.3 Legitimate Interests

Legitimate interests can be an operator's own interest or the interests of third parties, or even those of the players). The legitimate interests can include commercial interests, individual interests or broader societal considerations. This lawful basis may initially therefore appear as a 'catch all' lawful basis but, as with consent, care is needed on the part of operators to ensure that the scope and requirements are met before relying on it. The requirements are set out below with some practical examples:

- **Documentation and Assessment**

Operators wishing to rely on legitimate interests as a lawful basis must first complete a Legitimate Interest Assessment ('LIA'). This will allow the operator to assess and document whether, and how, this basis is appropriate and, in particular, to show that it has considered the balance between its interests and the interests and fundamental rights of the player.

Operators are expected under this Code to have in place appropriate LIA templates and processes. There is no specific form which must be used for an LIA (although some SAs such as the ICO in the United Kingdom do offer suggested templates which may be helpful). An LIA should cover the following:

1. A description of the methodology used in the LIA process, including any risk assessment methods applied.
2. The legitimate interest pursued by the operator in the personal data processing.
3. Precise details on the personal data which will form part of the processing.
4. A specific description of any processing that will be applied to personal data under this LIA. This must include:

- 4.1. the nature of the processing;
 - 4.2. what will trigger, or has triggered, the processing to occur;
 - 4.3. for how long the processing will continue;
 - 4.4. retention periods which are not covered by existing company policies, or the criteria to determine them;
 - 4.5. whether new technology is involved and, if so, details of that technology; and
 - 4.6. whether the processing is likely to result in a high risk to the rights and freedoms of players and, if so, details of those risks shall be highlighted.
5. An explanation of why the processing is necessary and proportionate to achieve the legitimate interest.
 6. A description of why this processing is within the reasonable expectations of the player¹, or an explanation of the compelling reasons justifying the processing.
 7. Any mitigating controls that will be implemented to manage risks to the player.
 8. How data minimisation has been achieved, including specific consideration of whether it is possible to offer opt-out to players.
 9. How any specific subset of personal data has been selected for this processing.
 10. Any benefits to the players in relation to the processing.
 11. Consideration of the players' interests, rights and freedoms.
 12. A statement on the period at which the LIA will be reviewed and a recognition that a significant change will also trigger a review.

- **The operator shall have in place appropriate LIA templates and processes.**
- **Before relying on the legitimate interest as a lawful basis, the operator shall complete a LIA.**
- **The LIA shall be reviewed at regular defined intervals and upon significant change to the factors which affected its conclusion.**
- **The DPO must be informed of any use of Legitimate Interests to support processing.**

- **Right to Object**

Players will have a right to object to an operator's reliance on legitimate interests and therefore to request that the processing is suspended or terminated.

This right is not absolute other than in the case of any direct marketing conducted on the basis of legitimate interests. With direct marketing, if an individual objects, the operator must take the necessary action e.g. stop the processing of personal data for this purpose. Most commonly, an individual will be exercising a right to object to direct marketing through an unsubscribe function or preference management center in any event, so there will be no need for a separate objection mechanism.

Outside of direct marketing, an operator will not be required to comply with an objection request if it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or if the processing is for the establishment, exercise or defense of legal claims.

¹ See Opinion 06/2014 of Art. 29 Data Protection Working Party on the '*Notion of legitimate interests of the data controller under Art. 7 of Directive 95/46/EC*', page 40.

Operators are required to inform players of their right to object. This should be done explicitly and presented clearly and separately from other information provided to the player – for example, it cannot just be buried in a privacy policy, but customers should also be notified of this right at the latest at the time of the first communication about that processing activity, where that is feasible (for example in marketing messages).

Example

A player is in a dispute with an operator about a breach of the account terms and conditions. The player writes to the operator and says they wish to exercise their right to object to any further processing of their personal data by the operator. Even though the operator has various correspondence and documentation with the player in relation to the dispute and is relying on legitimate interests to process it, the operator will not usually need to adhere to the objection where it has overriding legitimate interests to continue using that data to undertake the investigation and protect its business and defend itself.

Examples of possible processing activities where operators may be able to rely on overriding legitimate interests include (subject to appropriate assessment as set out above) the following:

- system testing and security measures;
- detection of player account fraud;
- analytics of trends and forecasting within the player database (assuming this is non-cookie based);
- investigating and bringing action in relation to breach by players of terms and conditions;
- necessary to target direct marketing where such communication is permissible under EU or any other Member State legislation;
- marketing activities where there is no specific obligation to have consent under local law (which is considered in more detail in case study in Part 0 of this Code);
- sharing the data with sports governing bodies and other organizations, for sports integrity purposes, which may also be justified under legal obligation or public interests;
- call recordings for quality assurance and for potential dispute resolution purposes;
- customer segmentation for the purpose of tailored promotions and bonuses sent via direct marketing e.g. knowing which customers are sportsbook customers, as opposed to casino customers;
- establishment of VIP status based on game history for the purpose of offering special benefits to customers;
- automated chat bot using AI to route customer queries/requests to the most appropriate personnel of the operator e.g. specific agents who can handle the request; and/or the chat bot asks a series of questions and provides answers without the need for human intervention. By processing personal data of customers, through AI, the chat bot is able to recalibrate itself to optimize its suggestions and answers.

➤ **The operator shall have implemented suitable procedures to respond to players' requests to object to processing operations based on legitimate interest.**

3.1.1.4 Special Category Data

Operators should usually only be holding special category data on players in very limited cases, but where they are, they will need to ensure that they have both an appropriate lawful basis for doing so under Article 6, and a separate basis for processing under Article 9, GDPR. Operators should be particularly attuned to local derogations and legal requirements and guidance at a country level when processing such personal data.

Example

A VIP informs their account manager that they will be in hospital and recovering for a month and provides details of the surgery they will have. The operator should consider whether it needs to process this personal data at all but, if so, it may wish to consider whether a lawful basis under Article 9 of explicit consent is applicable or that the individual has manifestly chosen to make this public applies.

- The operator shall appropriately document the lawful basis for the processing of any special category data.
- The operator shall follow any requirements at Member States level when processing special category data.
- The operator should consider any guidance at Member States level when processing special category data.

3.1.1.5 Criminal Offence Data

It should be only in exceptional circumstances that operators are processing criminal offence data in respect of players. To the extent that they are, however, operators will need to ensure that they have a lawful basis pursuant to Article 10 of the GDPR and comply with local law requirements which may involve the creation and maintenance of appropriate policy documents.

- The operator shall appropriately document the lawful basis for the processing of any criminal offence data.
- Such processing shall be supported by all required policy and process documents.
- The processing of any criminal records data shall be brought to the attention of the DPO.

3.1.2 Fair

This refers to the need for operators to ensure that they only use personal data in a way that is fair to players considering, in particular, whether any processing would be unexpected by, or detrimental to, them.

Example

If an operator collects personal data for ensuring compliance with money laundering requirements, this personal data should not then be used for direct marketing or profiling.

since this would not be 'fair' and would not be within the reasonable expectations of the player.

3.1.3 Transparent

This refers to the need to ensure that all relevant processing, the reasons for it, and the lawful reason supporting the processing has been declared to the player in an accessible and easily understood manner.

The principle of transparency is subject to certain exceptions. Specifically, operators are allowed to withhold disclosure of information to players about personal data processing, in cases where the disclosure may affect an ongoing investigation or even the operator's own obligations at law or compelling business interests. Such situations include but is not limited to:

1. details on a suspected offence or ongoing investigation (in order not to prejudice the prevention, investigation, detection and prosecution of criminal offenders by official authorities);
2. any suspicions or investigations on money laundering (as the disclosure of this information is tantamount to 'tipping off' which is offence under anti-money laundering ('**AML**') law);
3. risk assessments and logic behind profiling related to AML, terrorism financing ('**TF**') and fraud prevention monitoring (revealing this information would enable players to bypass these mechanisms);
4. risk assessments relating to, or the existence of and the logic behind, profiling or monitoring directly related to fulfilling responsible gambling ('**RG**') obligations (revealing this information would enable players to bypass these mechanisms);
5. logic behind, or detailed results of, risk assessment of players in sportsbook (revealing this information would prevent the operator from limiting its exposure to financial risk);
6. information about detection and cooperation for match-fixing and other sports integrity issues (revealing this information would jeopardize ongoing investigations, see the previous statement on the prevention and detection of crime);
7. the assessment or collection of a tax; and
8. other situations in which the law provides a clear obligation of confidentiality and non-disclosure or prevents any action capable of 'tipping off' (alerting) the subject of an investigation, or otherwise negatively impacting such an investigation.

Example

An operator is expected to explain in its player privacy policy that personal data may be processed for anti-money laundering purposes. However, it will not be expected to provide details of the logic behind its specific techniques for processing personal data for money laundering purposes, since this would be exempt from the disclosure requirements, as it would jeopardise the detection of crime.

Similarly, operators have a legal obligation to support responsible gambling, which they should declare in their privacy policy. As with the above it will not be expected to reveal the logic behind, or methods of, their actions to protect players as it would jeopardise the effectiveness of the activity.

Operators must be aware that such exemptions to the principle and obligations of disclosure are limited exceptions. An operator must be able to justify and document the reasons for relying on an exemption, for example, by demonstrating and documenting how the provisions exempting them from transparency apply to them and by informing players of their reliance on those provisions, when this would not be prejudicial to the purpose(s) of those provisions.

- **The operator shall fulfil its transparency requirements via privacy policies.**
- **The operator shall define in its internal policies how it will fulfil transparency requirements including an explanation of the exceptions.**
- **Any use of exceptions will be at the minimum level possible to achieve the purpose of the exception, it may not be necessary to make use of all aspects of the exception and where this is the case it shall be restricted.**

3.2 Purpose Limitation

This directly links with the 'fairness' principle. It is essential that a purpose for processing activities is understood and is clear from the outset, and operators must be clear and open about the reasons for obtaining personal data and what they will do with the personal data.

An operator who wants to undertake a new processing activity in relation to personal data must first check the purpose they collected the personal data for originally and what they informed players about that purpose. If the new purpose is compatible with the original processing purpose and would be expected by the player based on the information provided to them, the operator will be able to proceed. However, if the purpose is different to the original purpose and to what was communicated and expected by players, then the operator will need to consider afresh whether or not it has a lawful basis for this new processing and whether such processing meets the transparency requirements.

Example

If an operator has a player's phone number for account opening purposes, it cannot then start using the phone number for direct marketing purposes without separately determining whether it has a lawful basis for that direct marketing (for example, if operator can rely on legitimate interest exception from direct marketing). That would be a new, incompatible, purpose.

- **The operator shall be clear about the reasons for obtaining personal data and what it will do with the personal data.**

3.3 Data Minimisation

Operators should only process the personal data that is necessary for the purposes for which they are being processed. This means always asking the questions: do I need all this personal data for this specific purpose? Could I achieve the same processing with anonymous or pseudonymised personal data or with fewer personal data fields or data sample?

Data minimisation links directly to privacy by default and design (see section 7 below) meaning that these types of consideration should be designed from the outset of any new personal data processing activity. Where appropriate, the decisions made to demonstrate data minimisation should be set out in a Data Protection Impact Assessment ('DPIA') or LIA where these are required.

Example

An operator wants to run some analytics on the success of a recent marketing promotion. It should carefully consider whether any personal data needs to be processed for this purpose and if the outcome could instead be achieved by looking at aggregate anonymous statistics.

It is important to note that since online gambling is a very regulated industry, a huge part of operators' data processing activities are necessary per regulatory/compliance requirements (licensing requirements, gambling legislations, AML legislation).

Having in mind that, the very ratio of AML legislation and licensing requirements is to gather/keep as much as possible information, to be able to do a detailed analysis of potentially suspicious activities of players (from AML, TF, but also RG perspective). Therefore, AML and gambling legislations are based on the data maximization principle. On the other hand, the main principle of the GDPR is data minimization. Hence, it is essential to highlight this challenging role of operators in balancing these conflicting rights. Therefore, regulators should have in mind that operators must have a flexibility in collecting and processing personal data in order to fulfil very extensive AML/regulatory obligations.

- **The operator shall only process the types and quantity of personal data that is necessary for the purposes the operator aims to achieve.**

3.4 Accuracy

It is the responsibility of the operator to ensure that the personal data it controls is accurate and, where necessary, updated to accommodate any changes. This will involve ensuring that care is taken by customer support staff when recording player information correctly as well as providing players with easy ways to check their personal data, for example through their online account settings.

- **The operator shall ensure that the personal data it controls is accurate and, where necessary, updated to accommodate any changes.**

3.5 Storage Limitation

Personal data must not be kept by operators for longer than is necessary for the purpose for which it is being processed.

GDPR does not state how long personal data should be kept for, so it is up to operators to determine (and document their reasoning for) how long they are keeping personal data of players. This will require developing a data retention policy identifying the different periods personal data is kept for (in respect of each processing activity and on a departmental level) and then operationalising that within systems to ensure compliance. When the relevant retention period has been reached, then personal data should be deleted or anonymised.

In determining what is “necessary” as a retention period, operators will need to have consideration of:

- the legal obligations it is under to hold specific personal data and records for a specific minimum or maximum period, noting that these may vary in different jurisdictions;
- where there is no specific legal obligation relevant to the personal data and processing in question, what is appropriate and reasonable in the circumstances; and

- the specific lawful basis it is relying on for the processing and the bearing that has on retention periods, for example, when relying on consent the retention period should be tied to the period the consent remains valid for.

Example

Operators are specifically under an obligation in the EU to retain copies of personal data used for anti-money laundering purposes for no longer than required by national law after the end of the business relationship with a player or the date of an occasional transaction. Operators should, therefore, only keep such personal data for that specific period unless otherwise subject to a legal requirement to keep it for longer.

It is important to note that retention periods for customer data is one of the issues that requires industry-specific approach. This is especially important when determining the start of retention periods. For the accounts closed on customer request or closed by the operator, the retention period will start from the moment of closure of the account. However, the specificity of the industry is that customer does not have to close the account and it can be in inactive status permanently. Although from the regulatory/compliance perspective, this is fine, from a data privacy perspective, in accordance with the storage limitation principle operators should define when retention periods should start in this kind of situation. Operators will clearly define this in their retention policies or other relevant documents.

Another concern about retention periods, is for how long operators can retain data in accordance with AML laws. In some countries, AML laws define the minimum period for retention of customer data (for example, at least five years). In these cases where the law gives discretion to operators to define a maximum retention period, the legal basis for this is the law but the decision regarding retention periods must be supported by a documented risk assessment and reviewed at appropriate intervals.

In determining whether personal data needs to be retained beyond the years mandated by applicable AML laws, operators must be able to provide a reasonable justification (as explained below in the case of customers with multiple accounts²).

- **The operator shall develop a data retention policy identifying the different periods personal data is kept for (in respect of each processing activity and on a departmental level).**
- **The data retention policy developed shall take account of the requirements set in other laws, e.g. AML laws.**

3.6 Integrity and Confidentiality

This is the high-level principle that personal data should be processed with appropriate information security. Requirements in respect of information security are covered in more detail in section 6 below.

4. DATA SUBJECT RIGHTS

This section covers the various rights individuals have under Articles 13 to 18 and 20 to 22, GDPR and specific considerations for operators in relation to the exercise of such rights.

It is important for operators to take these rights very seriously and respond to requests within the relevant deadline. When handling these requests, it is crucial to have good customer service

² See section 4.4 of the Code.

strategies and procedures to ensure that the identification and response to the requests is managed effectively.

It is useful to think about a request in relation to player rights under GDPR through the following specific questions:

- Does the operator process any personal data of the requestor?
- Is it a valid request?
- What processing activities and personal data does the request cover?
- What is the lawful basis for processing that you are relying on (since that may impact whether the request actually arises)?
- Are there any exemptions which may apply to the specific request?
- What information needs to be given to the player in response to the request?
- When is the deadline for responding?

The GDPR provides individuals with the following rights: right to be informed; right to access; right to rectification; right to erasure; right to restriction of processing; right to data portability; right to object; right not to be subjected to solely automated individual decision-making which produces legal or similar significant effects on the player, including profiling. Each of these is considered below with practical considerations for operators.

4.1 **Right to be Informed**

Under Articles 13 and 14, GDPR, players have the right to be informed about the collection and use of their personal data. The right to be informed relates to the transparency principle in the GDPR and discussed in section 3.1.3 above requiring that information relating to the processing of their Personal Data is presented to players in a clear and concise manner.

In nearly all cases, operators will largely be fulfilling this requirement through a privacy policy which is clearly presented to players at the point of account registration and which is always present on the operator's website or within the relevant app for reference by players or potential players/visitors. Operators can also provide information through other means, when requested by the player, or through the design of the services, for example, through the use of pop up information. Operators must consider carefully the way in which the information is provided, to ensure that it is clear and helpful to the players. In particular, the use of plain and easy to understand language, giving examples and also considering other forms of layered notice or additional forms of presenting information, such as the use of infographics or videos, can be helpful.

➤ **The operator shall present a privacy policy to the players during the registration of the account. The privacy policy shall be always accessible on the operator's website or app.**

4.2 **Right to Access**

Under Article 15 GDPR, players have the right to access a copy of their personal data as well as to receive certain other supplementary information about the processing of their personal data. These requests are commonly referred to as Data Subject Access Requests ('**DSARs**') or Subject Access Requests ('**SARs**').

Operators will need to develop processes and procedures to enable them to respond correctly and in a timely fashion to DSARs. When allowed by national law, operators can request ID

verification from the player, before disclosing the data requested. Operators need to bear in mind the following practical issues:

- Players are only entitled to receive a copy of their own personal data, not that of other people, and therefore, operators will need to review personal data in order to extract just the personal data relating to the player making the DSAR or to redact the personal data of third parties.

Example

A player makes a DSAR and specifically requests copies of all chatroom data. The operator will need to go through the chatroom logs and either extract and only provide the personal data relating to that player (for example, comments/notes about them by the operator will not be part of DSAR), or the operator could choose to redact personal data in the chatroom that does not relate to the player and is not their personal data.

If the chat only concerns the player and the chatroom host, the operator may find it simpler to give a copy of the whole log but should consider any impact this may have on the chatroom host and their personal data.

- There are exemptions to the right to access which may be relevant in certain situations. For example, operators may need to withhold or redact information on a case by case basis where it is subject to a legal requirement not to provide the personal data, or the information is subject to legal privilege (for example in some circumstances relating to correspondence with an internal or external legal advisor). The exemptions available vary at a Member State level. More information about common exceptions in this industry are provided in Chapter above 3.1.3.
- If it is not clear what the player is requesting, the operator may wish to consider whether it is helpful to quickly revert back to the player and ask them to clarify what exactly it is that the player is requesting. Seeking clarity on a request may also narrow the scope of the information that the player is looking for and be more helpful to the player by focussing on the specific information they require.
- Operators cannot require that DSARs are submitted in a particular way or in a particular form, although providing such forms or clear specific email addresses may be helpful to help funnel such requests and enable players to get a response faster. Operators will therefore need to ensure that its customer services teams are trained to spot and escalate DSARs that may be received in through other more general channels.
- Given the tight timeframes for responding to DSARs, operators should have a log to record the requests received in order to identify relevant deadlines and to comply with the principle of accountability.
- Where possible, operators should consider whether they can provide remote access to a self-service system which would provide the individual with direct access to his information even if only for some commonly requested data such as past transaction records.

➤ **The operator shall have a defined and documented procedure to respond to DSARs.**

➤ **The operator shall ensure that its customer services teams are trained to identify and escalate DSARs.**

- **The operator should record all the DSARs received in order to comply with the accountability principle.**

4.3 Right to Rectification

Under Article 16, GDPR, players have the right to have inaccurate personal data rectified. Personal data is 'inaccurate' if it is incorrect or misleading as to any matter of fact. It is important to note that in this industry usually operators will not be able to provide players with a way of checking and updating personal data themselves by logging into their account and using functionality there to make amendments, because of the AML/Know Your Customer and other legal verifications that operators need to perform within the scope of their legal obligations. This is why operators should define in relevant policies the process for exercising this right, taking into account specifics of this industry and operator's business model.

If the operator is satisfied that the personal data in question is accurate, it should explain to the player its decision to maintain the information, create an audit trail of such decision and inform the player of their right to make a complaint to the relevant SA. Operators should inform third parties about the rectification of personal data if the operator has transferred the player's data to third parties (e.g. regulatory bodies, suppliers, joint controllers), unless this proves to be impossible or involves a disproportionate effort.

- **The operator shall provide players with a way of checking personal data and establish a process to exercise this right, in accordance with their data rights and regulatory compliance obligations.**
- **Where the operator decides not to update the personal data of the player, they must explain this reason to the player, unless an exemption applies.**

4.4 Right to Erasure

Under Article 17, GDPR, players have the right to have their personal data erased. This is commonly known as the 'right to be forgotten'. It is crucial to note that this is not an absolute right and applies only in certain circumstances.

In the context of the online gambling industry, it is important to balance the rights of the players with the respective operator's obligations under other areas of law, such as those under relevant tax and gambling regulations, as well as potential legal claims. The full list of the exemptions to this right can be found in Article 17(3), GDPR and applicable Member State law. Highlighting these exemptions to the requesting player in responding to the request for erasure will help the requestor to understand the operator's overriding legal obligations. Operators will define in their internal policies reasons due to which data cannot be deleted.

Operators shall inform third parties about the erasure of personal data if the organisation has in fact transferred the player's data to third parties, unless this proves to be impossible or involves a disproportionate effort.

Example

A player closes their account and tells the operator that they want all of their transaction data erased. The operator will not be able to erase this personal data because, even though it is no longer providing the service to the player, it must retain a copy of the transactions to comply with relevant legislation and to assist it in investigating any complaints and defending or bringing any relevant legal claims.

In addition, here is important to explain another specific concern for the industry. As stated before, in the industry there is a trend of regulators to impose on operators broad and extensive obligations regarding AML, RG, and fraud checks. All these measures require operators to take preventative steps and analyse a broad scope of customers' data/activity to detect problematic behaviour at an early stage. Operators that have multiple brands should be able to analyse activities and data of customers across all these brands. However, the issue is when operators need to decide if to delete data about one customer account because the retention period expired, while the same customer has another active account on other operator's brands. Deleting data from one account, while we still should monitor this customer on other accounts, might have negative implications on the quality of the data analysis.

In these situations, if all these brands are within the same group of companies, operators should be able to retain data from other accounts if customers have at least one active account and the data from closed accounts are relevant for analysis of customer activity per operators' risk-based approach. For example, the player is classified as high risk, or it had some suspicious activities due to which it has to be monitored. Therefore, retention periods in the situation of multiple accounts can start from the closure/inactivity of the last active account.

- **The operator shall define in its internal policies the exceptions for which certain data cannot be deleted using the right to erasure.**
- **The exceptions mentioned above shall be mentioned to the player in responding to the request for erasure. The operator can either refer to the privacy policy or explain the exceptions specifically to the player.**

4.5 **Right to restrict processing**

Under Article 18, GDPR, players have the right to restrict the processing of their personal data in certain circumstances. This should not be confused with the right to erasure as this particular right only limits the ways in which the operator can use their personal data but does not involve deletion. When the processing has been restricted, the personal data shall, with the exception of storage, only be processed with the player's consent or for certain other exemptions as provided by the GDPR.

Operators should implement mechanisms to enable the restriction of certain types of data or for certain purposes if required. An operator shall inform third parties about the restriction of personal data if it has in fact transferred the player's data to third parties, unless this proves to be impossible or involves a disproportionate effort.

- **The operator shall implement mechanisms to allow the restriction of processing of certain types of data.**

4.6 **Right to Data Portability**

Under Article 20 of the GDPR, players have the right to require an operator to send their personal data to another data controller, for example another operator, or directly to the player. The right to data portability is intended to allow individuals to obtain and reuse their personal data for their own purposes across different services.

Operators will have to provide only personal data processed for the performance of the contract or based on player's consent, as long as the processing is carried out by automated means. As an example, this includes personal data submitted by the player upon registration.

The right to data portability does not include personal data where the lawful basis for the processing is not consent or contract, for example, data which is processed for legitimate interests or legal obligation. Exempt data that cannot be ported may include, but is not limited to:

- results of an algorithmic analysis of the player’s gaming behaviour;
- player’s profile kept by operators in the context of risk-management and financial regulations; and
- player’s data processed as part of the operators’ obligations to prevent and detect money laundering and financial crimes, and manipulation of sports competitions, where stipulated by law.

Example

A player requests that an operator port all of their account data to another operator and specifically wants to ensure that the new operator will offer them exactly the same bonus arrangements.

The transferring operator must provide personal data such as account registration, transaction history and marketing preference (if consent based) data but it does not need to provide the new operator with details which are not processed under the lawful reason of consent or necessary for contract, for example, the analytics it has used to determine the bonuses that are offered to the player.

The right to data portability entitles a player to receive a copy of their personal data and/or to have their personal data transmitted from one operator to another operator in a safe and secure way, without affecting the usability of the data. As a best practice, operators may also consider utilising a portal from which the player can directly access and export this personal data at any time, doing so would meet the requirements of data portability.

In light of the principle of data minimisation, it might be expedient that the disclosing operator directly contacts the receiving operator, to determine which types of data are required by the latter and which format is best suited. However, the decision to opt for this approach shall rest with the player and shall not affect the principal obligation of the operator to provide another operator with the full data set as described above.

The specific format of the transmission is not covered by the Code and shall be agreed on a case by case basis between the operators, but personal data must be provided in a format that is:

- structured (the structural relation between elements is explicit in the way data is stored);
- commonly used (the format is widely used and well established); and
- machine-readable (the format shall be automatically read and processed by a computer).

Operators shall have in place documented procedures in respect of portability and which shall contain as a minimum, details of:

- the kind of structured, commonly used and machine-readable format of the transmission; and
- the secure methods of the transmission.

➤ **When requested by the player, an operator shall provide his personal data to another operator. The disclosing operator should contact the receiving**

operator to determine the details on the types and format of data to be transferred.

- The operator shall have in place documented procedures on data portability with the minimum requirements set above.

4.7 Right to object

The right to object has been considered in the context of the legitimate interests' lawful basis in section 3.1.1.3 above.

4.8 Right not to be subjected to solely automated decision-making including profiling

Article 22, GDPR grants the player the right not to be subject to a decision solely made on the basis of an automated decision including profiling which produces legal or similarly significant effects on the player, and to be given certain information in relation to the process and decision. This will require an operator to assess and determine:

- if and when it is profiling by using solely automated processing or making solely automated decisions about a player based on the definitions in GDPR; and
- what rights the player has in relation to such decisions and how it will operationalise the individual's rights.

Each of these is considered in turn below.

4.8.1 Definitions

As computer systems evolve, in both speed and their ability to model decision making practices, it becomes increasingly cost effective to automate certain key decisions. This provides benefits to both the operator and the player, including speed, repeatability and consistency. In a similar way, profiling can be used for a variety of reasons, including tailoring website content to an individual's interests or ensuring that they only receive relevant information.

These systems also come with risks. Not all situations match a predetermined set of rules and, if the system misidentifies the data subject, their interests, or their patterns of behaviour, then any decision is fundamentally flawed. Moreover, these processes can be quite opaque as players might not know that they are being profiled or understand what that involves.

Operators will need to consider carefully if their activities, including profiling, consist of automated decision making with meaningful human involvement, or solely automated decision making. These are key distinct concepts.

- The operator shall assess if its processing of personal data constitutes automated decision-making, solely automated decision-making or profiling.

(i) **Automated and Solely Automated Decision Making**

Automated decision-making is the ability to make decisions by technological means based on data provided directly by customers; data observed about customers; derived or inferred data (e.g. risk rating).

It is key to differentiate decisions that are automated from those which are **solely** automated. All relevant processes must be mapped out, documented and the risk must be assessed. Decisions that are solely automated pose the highest possibility of risk to individual data subjects and will generally require a DPIA to be completed.

For any type of processing to be classed as automated rather than solely automated, there must be **meaningful human involvement** in the process (for example through review or filtering) and that human involvement must take place prior to the final decision. As an extreme example, if a person was employed to simply click “accept” on every recommendation a computer makes, this would still class as solely automated processing. Fig. 1 below gives a flow diagram for differentiating between the two concepts.



Example

An operator uses technology to help identify patterns of stakes by players that may be indicative of fraud and could mean that the player’s account should be suspended. If the operator still has staff checking the patterns and recommendations of the tool and making the decision whether or not an account should be suspended, then this is not a decision that is a solely automated decision.

(ii) Profiling

Profiling is any form of automated processing of personal data consisting of the use of personal data gathered from various sources to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s economic situation, personal preferences, interests, reliability, behaviour, location, etc.

The concept of profiling is related, but not identical to, the notion of both automated and solely automated processing. Automated and solely automated decision making may well comprise profiling but this is not always the case, as decisions can be made with or without profiling. Also, profiling can take place without making automated decisions based upon it.

To fall within the definition of profiling, processing must:

- involve automated processing, but may also contain human elements;
- be carried out on personal data, including identifiable information that enables the evaluation of personal aspects of a player; and
- have the objective of evaluating personal aspects of a player, and usually, but not exclusively, involves the following elements:
 - data collection;
 - data analysis to identify patterns and correlations to other data;
 - use of the analysis to anticipate characteristics of a player or their behaviour.

It should be noted that a simple classification of customers based on specific characteristics does not necessarily lead to profiling if the purpose is not to assess individual characteristics.

Example

If the operator wants to classify its customers according to their age or gender for statistical purposes and to acquire an aggregated overview of its customers without making any evaluations, predictions or drawing any conclusions about the customer, this will not be deemed as profiling.

All profiling operations must comply with the GDPR requirements in full, with particular attention to the principles of fairness, purpose limitation and transparency. The GDPR requires operators to provide customers with information on the existence of automated decision-making, including profiling and at least in those cases, “meaningful information about the logic involved”, as well as the significance and the envisaged consequences of such processing for the data subject. However, operators must be careful to draw a balance between adhering to their transparency obligations and protecting intellectual property and commercially sensitive information.

By providing too detailed information on the logic (including propriety algorithms or the know-how that underpins the process), operators are precluded from fulfilling their legal obligations by allowing customers to exploit mechanisms aimed at the protection of the operators’ business. For example, in the case of profiling for fraud/crime prevention purposes as well as players protection (based on law or public/legitimate interest), operators cannot provide players with the logic behind this because that would enable players to bypass the controls. The same goes for automatic decision making.

➤ **The operator shall provide players with information on the use of automated decision-making, including profiling.**

➤ **The operator shall establish the degree of detail of the information provided to the player in relation to automated decision-making, in order to not hinder its compliance with other legal obligations.**

4.8.2 Player rights in respect of automated decisions and profiling

Whilst the GDPR data subject rights apply generally to all processing, there are specific additional rights targeting solely automated decision-making. Specifically, a player will have the right to:

- **Not be made subject to a solely automated decision which produces legal effects on them, or which similarly significantly affects them**

In effect, this means that an operator cannot carry out solely automated decisions which would have such an effect unless it is able to fulfil one of the specific criteria set out in GDPR. Specifically, the decision must be:

- necessary for entering into, or performance of, a contract;
- authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- based on the data subject's explicit consent.

In the gambling industry, an automated decision is said to have legal effect if, for example, it results in the player being subjected to surveillance by a competent authority. On the other hand, an automated decision is said to similarly significantly affect the player if it has the potential to influence the circumstances, behaviour or choices of the player.

Example

An operator uses machine learning tools to run 'know your customer' checks on new players, to speed up the process of registration. If this is necessary for the performance of the contract or required under local law, the player will not have a right to reject the decision made by such checks. This also includes tools used to geo-block registration from certain countries due to regulatory requirements, for blocking Politically Exposed Persons ('PEPs') and IPs from countries under sanctions.

Example

An operator uses technology to identify its most loyal players to offer a bonus promotion to. Whilst this is a solely automated decision, the offering of a promotion would not have a legal effect or otherwise similarly significantly affect the player, so they will not have a right to reject it.

- **To obtain an explanation of the decision reached after such assessment**

As already explained above, the operator should find simple ways to tell the customer about the rationale behind, or the criteria relied on in reaching the decision. What is mandatory is sufficient insight into the logic and the significance of that logic so that the customer would have the necessary context to make an informed decision on whether to object. This does not apply to the previously mentioned circumstances where operators are precluded from providing information on the logic in order to adhere to their legal obligations.

- **To contest the decision and seek human intervention**

Safeguards that must be put in place around solely automated decision-making require operators to have a method for players to contest the decision and to require direct human review or intervention.

➤ **The operator shall provide players with an easy way to exercise this right.**

- **The operator's staff reviewing the decision must have the appropriate seniority to change the outcome if this is the conclusion of the review.**

5. **DATA SHARING AND TRANSFER**

5.1 **Scope**

This section 5 provides clarity and guidance on the principles for disclosing data to different recipients. It covers transfers by operators to other data controllers or to data processors (in each case whether external or internal within the operator's corporate group and whether or not the other entity is a private company or public authority).

GDPR contains different obligations depending on whether a transfer is to a data processor or to a data controller as explained below and operators must also consider whether any transfer is to an entity based outside of the European Economic Area ('EEA') since further considerations then apply in addition.

5.2 **Sharing With and Transfer to Data Controllers**

When managing a relationship with another data controller, an operator must first determine the nature in which it and the other controller is acting. Specifically, it must assess whether the processing involves transferring:

- between data controllers on the basis of each controller being a separate data controller (i.e. each controller is separately determining the purposes and means of processing); or
- on the basis of the controllers being 'joint controllers' (i.e. jointly determining the purposes and means of processing).

For all data sharing, whether under (i) or (ii), an operator will also need to consider the following:

- **If the sharing will be systematic, routine and repetitive or exceptional or one off**

Systematic sharing will usually involve routine sharing of data sets between operators and third parties for a pre-arranged purpose.

Operators may also decide to, be asked or obliged to share data in situations which are not covered by routine procedures or agreements (e.g. police requests).

- **Identification of a lawful basis for the processing**

As with any processing, the operator will need to ensure it has a lawful basis for the processing (as discussed in section 3.1.1 above), here being the transfer of personal data to another data controller.

Example

Operators may be asked to share personal data with sports bodies in the context of detecting match-fixing, self-betting and other sports or gambling related offences and crimes.

For non-special category data, the appropriate lawful basis will likely be legitimate interests (subject to an appropriate legitimate interests assessment). In the case of special category data, most Member States allow for substantial public interest grounds which will be relevant here, but the operator will need to consider the local Member State restrictions and limitations on such processing.

In addition, some sports organizations have their own rules that regulate sharing of data for these purposes, between its members.

Example

An operator wants to share personal data with another operator to enable a cross-email marketing campaign. The operators will need to factor in the requirements for consent as a lawful basis, including that consent will need to have been specifically obtained for use by the other operator by name.

Due to the nature of the industry and AML risks, operators frequently receive requests by different organizations to share personal data of players for purposes that are defined by law or in public interest (detection and prevention of different types of crimes). When it comes to police requests and other requests from governmental institutions, it is important to note that as controllers they are also responsible for the legitimacy of these requests.

First, this is due to the fact that the institutions are in the best position to estimate when they can request specific data. Moreover, due to the confidentiality of these investigations, they cannot provide a full explanation on why they need the requested data. For that reason, operators should act upon these requests, if the request contains the minimum necessary information: an explanation of the reasons for requesting the data; specification of data requested; and where possible a legal basis should be specified as well.

➤ **When sharing data with another controller, the operator shall assess if the processing involves transferring between two independent data controllers or between joint controllers.**

- **Data minimisation and security**

Operators should ensure that the scope of the personal data that is shared is only that which is necessary for the required purpose. The operator should consider whether techniques such as pseudonymisation, anonymisation and encryption and hashing are appropriate to limit or protect the personal data.

➤ **The operator shall ensure to share only personal data needed for the required purpose.**

➤ **The operator should assess if its security measures are appropriate to protect the personal data during the sharing.**

- **Documentation**

For routine data sharing, operators will need to put in place data sharing agreements or policies that explain the legal basis for data sharing with the third party and the obligations of each party in relation to the data sharing activities. Operators must bear in mind that, if sharing is on a joint controller basis, this arrangement will need to incorporate the requirements of Article 26, GDPR, in particular. As a minimum, such an arrangement pursuant to Article 26 should clearly indicate: (i) which controller will deal with the players' requests (this shall also be communicated to the players); and (ii) their respective responsibilities under the data protection laws.

As for the agreements between independent controllers, although GDPR does not define the mandatory elements of such agreements, operators, as a good practice, may enter into data sharing agreements, to at a minimum protect the data of players and define the roles of the parties.

For intra-group transfers, operators will usually need to have in place an intra-group transfer agreement (or explain other legal basis for data sharing in the relevant policy) as transfers between different group members requires a legal basis and therefore must be regulated in a similar manner as other data transfers.

For one-off data sharing, it may not always be possible to put in place the same type of documentation but an operator will, nonetheless, need to record its grounds for the data sharing.

- **Transparency**

Operators are required to inform players about recipients or categories of recipients of their personal data, for example via the player privacy policy, unless an exemption applies.

- **The operator shall define its data sharing framework that will define operator data sharing with third party controllers.**
- **The operator shall have agreements or policies to manage intra-group transfers of personal data.**
- **The operator shall inform players about recipients or categories of recipients of their personal data through its privacy policy, or equivalent.**

5.3 **Sharing With and Transferring to Data Processors**

A data processor is the natural or legal person, public authority, agency or other body which processes personal data *on behalf of* the operator. The types of processor and manners of regulating the relationship may be as varied as the types of services that involve access to personal data, but the key is that it is the operator which decides the purpose of the processing and use of the information, while data processors only carry out the instructions of the operator.

Processor arrangements are most commonly found for operators in the context of service providers (for example companies that provide to the operator services, such as information storage service in their servers).

Example

An operator engages a software contractor to undertake some development work on its player database and to its instructions. The contractor will only have access to personal data in providing the services. It will be a data processor.

Even though processors are subject to GDPR directly, operators have certain obligations they must follow when working with and transferring personal data to processors as set out below.

5.3.1 **Selection of Data Processors**

Operators must only use processors that provide sufficient guarantees to implement and maintain technical and organisational measures to ensure that all processing will meet the requirements of the GDPR and protect players.

As a result, the operator has a duty of diligence when choosing the data processors and will need to assess (and document) their selection. Considerations in an assessment should include:

- security arrangements (technical and organisational) of the processor;
- the location of the processor and where they will hold and transfer any personal data;
- the processor's ability to comply with data subject rights requests; and
- if possible, evidence of GDPR's compliance;
- any adherence to an approved code of conduct or an approved data protection certification mechanism to the extent available.

The extent of the assessment required will depend on the processing activity that the processor will be undertaking, and the risks associated with that processing.

Example

An operator will need to carry out much more detailed assessments on a processor that will be supplying fraud monitoring software services than a processor that will be conducting analytics on a small pseudonymised dataset, since the nature and extent of the data processing carry different risks. In each case, the operator's data protection compliance and information security teams will need to work together to ensure the assessment is appropriate and documented.

5.3.2 Contractual Documentation

Operators must ensure that they have appropriate contractual protections in place with a processor. This must be in writing and legally binding. The data processing agreement must include (as a minimum) the requirements contained in Article 28(3)(a)-(h), GDPR, that is: the duration of the data processing agreement; clauses regarding the processing of the personal data; confidentiality obligations for persons authorized to process personal data; the conditions of sub-processing, if allowed; the personal data breach handling and notification; the deletion of personal data; the audit rights; the subject matter and duration of the processing; transfers of personal data outside the EEA; the nature and purpose of the processing; the type of personal data to be processed; the categories of data subjects and the obligations and rights of both parties.

- In particular, operators should ensure that any data processing agreement clearly sets out details of the processing operations over personal data within scope;
- states the expectations of the operator in terms of how the personal data will be processed and that the processor must not process the personal data outside the scope of the operator's instructions;
- is updated to reflect any significant and substantial changes in processing taking place, for example, the scope of the data is significantly different from the original scope agreed by the parties;
- provides for appropriate level of security which may include the addition of specific detailed security commitments on the part of the processor;
- requires that a processor shall communicate any legally binding request for disclosure of the personal data by a law enforcement authority to the operator, unless otherwise prohibited; and

- requires that the processor must obtain the operator's written specific or general authorisation prior to engaging any sub-processor. If the operator relies on general authorisation, it shall implement a robust monitoring process, which includes notification of the appointment of any sub-processors and any changes to the sub-processors.

5.4 Transfers out of the European Economic Area

When transferring personal data to another data controller or data processor, operators have to be mindful about the personal data transfers to third countries (countries outside the EEA) that do not provide for an adequate level of protection and therefore need to be covered by appropriate safeguards.

The safeguards which will be most appropriate to operators are:

- binding corporate rules (where a member of the corporate group of a licensee is established outside the EEA. If in place, this must be evidenced and cover the relevant scope of the processing);
- Standard Contractual Clauses³ (also known as the model clauses of which there are versions for transfers to processors and to controllers);
- consent, but this is only applicable for one off non-routine transfers; and
- in limited situations where a court or any administrative authority from a third country requires the transfer of personal data from the EEA and there is an international agreement between the requesting third country and the Union or a Member State (e.g. judicial cooperation), operator will share requested data with the local authority, in accordance with the international mechanism for cooperation in criminal and judicial matters.

Example

A global operator has entities in Europe, the US and Asia. It wants to allow for the transfer of personal data between some of these entities for analytics and fraud detection purposes. The operator could consider entering into binding corporate rules but this is an extensive exercise which will take considerable time to put in place. The alternative is to put in place an intra-group transfer agreement including Standard Contract Clauses for any transfers by its European operations to the US or Asia based entities.

- **The operator shall document in the relevant internal policy how due diligence assessment of data processors will be conducted.**
- **The operator shall use only processors that provide sufficient guarantees to implement and maintain technical and organisational measures to ensure that all processing is compliant with GDPR.**
- **The operator shall have in place a data processing agreement with the processor. The data processing agreement shall contain the minimum**

³ Decision 2001/497/EC <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32001D0497>, Decision 2004/915/EC <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915> and Decision 2010/87/EU <http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087>, until the current Decisions will be replaced by new Regulations.

requirements of Art. 28(3)(a)-(h) GDPR and should include the best practices mentioned in section 5.3.2.

- The operator shall document decisions about the choice of transfer mechanisms in the relevant policy.

6. **SECURITY AND DATA BREACH NOTIFICATION**

6.1 **Scope**

As a general rule, Article 32, GDPR requires controllers and processors to adopt a risk-based approach to security measures “to ensure a level of security appropriate to the risk”. This means assessing the potential risks inherent in a particular activity, identifying and implementing mitigation techniques to control and reduce to an acceptable level the risk of such activity.

6.2 **Security Measures**

The specific security measures that operators should consider implementing to meet the requirement under Article 32, GDPR include:

- Pseudonymisation and encryption of personal data (to protect data being modified by an unauthorised party). This is considered in more detail in 6.3 below.
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident, as well as document regular reviews of access controls.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing, providing staff awareness and training and ensuring that data can be accessed in a timely manner in the event of an incident.
- Operators may also use certification mechanisms as a part of demonstrating compliance with the obligations set out above (for example ISO 27001, which is recommended by various SAs).

In determining the appropriate security measures to be implemented, operators must have regard to:

- The state of art and the costs of implementation. There is no definition of “state of the art” within the GDPR but it can be regarded as an attempt to account for future technological advances and also allows for cost to be a factor in determining the appropriate level of security. However, this does not mean that the latest technology is required.
- The nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of players.
- The risks that are presented by data processing in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

6.3 Pseudonymisation

This is a procedure by which personal data fields within a data record are replaced by one or more identifiers or pseudonyms so that linkage to a player is not possible without additional information that is held separately, impeding re-identification. The risks associated with data processing are therefore, significantly reduced.

Example

Using a player ID can be a useful way for operators to minimise the personal data used by it for a particular purpose where personal data cannot be anonymised. A player ID is a form of pseudonymisation: the operator still has the means to link the player ID to an individual player but a list of player IDs in itself does not do that directly and so helps minimise personal data exposure and use.

Even though the use of pseudonymisation increases the level of security, it is not intended to preclude any other measures of data protection according to Recital 28, GDPR. Therefore, operators shall implement pseudonymisation as part of an overall 'Information Security Management System' (or ISMS).

The EDPB has described pseudonymisation as a useful security measure and also provided some examples of techniques in its guidance, including hash functions and tokenisation.

Pseudonymisation is a key feature of the concepts of privacy by design and by default and it can help reduce the risks to players, as it provides an additional layer of security for an individual's data. Operators should consider the application of pseudonymisation when possible as part of an organisation's risk minimisation strategy; such application shall also include strong controls around access to data that re-identifies the player. Although pseudonymisation presents the risk of potential identification of individuals with data from one or more sources being combined or matched with pseudonymised data, this method will assist to reduce any potential risk. It is important to note that personal data that has been pseudonymised – e.g. key-coded – cannot be used to identify an individual, depending on whether it is possible to attribute the pseudonym to a particular individual. Therefore, in some cases pseudonymisation can totally reduce the risk of identification.

6.4 Confidentiality, Integrity, Availability and Resilience

To ensure a high level of security of systems and services, as a matter of best practice, operators should consider the following:

- Documented, regularly reviewed and effective access controls protecting personal data from unauthorised access or disclosure. This would include the use of strong encryption tools and training of employees privy to such personal data.
- Ensuring that personal data is accurate throughout its life cycle and protected from being modified by unauthorised parties.
- Ensuring that personal data is available when needed.
- Physical security measures as well as technical, for example, CCTV, locked facilities, confidential waste disposal and physical security of devices are all as important to review as technical measures such as firewalls, encryption and vulnerability scanning.
- The importance of the human, and human process, element of security.
- Article 32(1)(c), GDPR requires an operator to be able to restore availability and access to data in a timely manner in the event of a physical or technical incident. In order to

comply with this, an operator should have taken into account the types of processing and risks involved and document findings.

- The requirement of Article 32, GDPR extends beyond IT security and technology measures to organizational controls as well. Operators should include organisational measures, including training of employees and ensuring appropriate governance frameworks and access control protocols are in place.

6.5 Testing

Article 32(1)(d), GDPR requires regular assessment and evaluation of the effectiveness of technical and organisational measures for ensuring the security of data processing. Such tests could include:

- regular monitoring for security issues and testing of business continuity/disaster recovery plans on a regular basis;
- regular testing of the effectiveness of organisational measures; and
- ensuring employees are signed up to confidentiality provisions.

- **The operator shall adopt a risk-based approach to security measures. Certification mechanisms can be used to demonstrate compliance with the obligations set out in section 6.2.**
- **The operator should implement the specific security measures of section 6.2.**

6.6 Data Breach Notification

One of the key changes implemented by the GDPR is the requirement for mandatory notification of data breaches to the relevant SA(s) and affected individuals. These new obligations are essential to the principles of accountability and transparency that run through the GDPR. This section 6.6 outlines the definition of a personal data breach and the thresholds for notification.

6.6.1 Definition of Personal Data Breach

A personal data breach occurs where there is a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, transmitted, stored or otherwise processed.

The most commonly used model for managing information security within an organisation is represented by the 'CIA' triad of information security, which is centred in three key areas related to information systems, including Confidentiality, Integrity and Availability. Based on this model, personal data breaches can be classified in three different categories:

- **Confidentiality breach:** an unauthorised disclosure of, or access to personal data;
- **Integrity breach:** alteration or unauthorised changes of personal data;
- **Availability breach:** loss, accidental or unlawful destruction or loss of access to personal data.

A personal data breach could simultaneously affect the confidentiality, integrity and availability of personal data.

Example

An operator experiences a temporary loss of personal data that is properly encrypted and unintelligible for third parties. This is an availability breach.

Examples of personal data breaches could include any of the following, which lead to an impact on the personal data of the player:

- loss or theft of data or equipment on which identifiable personal data is stored;
- unauthorised use of personal data due to inappropriate access controls;
- equipment failure that caused destruction of personal data;
- human error that revealed personal data to unauthorized recipients;
- complete destruction of customer database;
- unforeseen circumstances such as a fire or flood that destroyed personal data;
- a cyberattack that exposes names, addresses, dates of birth and encrypted passwords of players;
- social engineering offences where information is obtained by deceiving the organisation who holds the records;
- sending or disclosing personal data to an incorrect recipient;
- a significant disruption to the normal service of an operator due to power shutdown which caused unavailability of personal data.

6.6.2 Breach Response Plan

Operators must have in place a documented data breach response plan for dealing with a security incident and the identification and handling of any personal data breach to enable it to take the appropriate steps deemed necessary to identify, contain and mitigate its possible adverse effects and resolve any incidents. Such a plan should involve and include:

- The response team should be composed of cross functional members, which includes the DPO or a member of their team, to prevent, identify, address and provide immediate and effective response to any unexpected event involving the unauthorised disclosure, loss or destruction of personal data.
- Responsibilities and authorities should be assigned to key individuals within the organisation.
- Procedures for identifying, categorising and communicating personal data breaches. After becoming aware of a potential security incident, operators shall carry out a preliminary investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation, operators may not be regarded as being “aware”. Operators will be considered “aware” of a breach, which initiates the 72 hours timeframe to notify the SA, as soon as it has a reasonable degree of certainty that a security incident has occurred, and that personal data are compromised.
- The methodology for carrying out a breach severity assessment and accordingly notify the competent SA as well as the affected individuals.

- Appropriate procedure of notifying the SAs and players of the personal data breach, if needed (as considered in more detail below).

6.6.3 Containment

Once it has been established that a personal data breach has occurred, operators shall take immediate and appropriate action to limit the breach. Operators shall evaluate:

- Who within the organisation needs to be made aware of the breach and inform them of what they are expected to do to contain the breach.
- Document the risk assessment of the data breach.
- Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause.
- Establish whether the competent SA needs to be notified where the breach amounts to a risk to affected individuals.
- Establish if it is appropriate to notify affected players immediately (e.g. where there is a high level of risk of serious harm to players per risk assessment performed).
- Where appropriate (e.g. in cases involving criminal activities), inform the police.

6.6.4 Processors

The GDPR places direct obligations on data processors as well as data controllers. Data processors must report personal data breaches to operators without undue delay. Where personal data processing has been delegated to data processors, operators would be considered to be aware of a breach once the processor has made the operator aware of the breach and the operator will need to consider its own notification obligations.

Operators must ensure that data protection clauses in contracts with their data processors are in place to define the processors' obligations during the duration of the contract. These clauses shall provide that:

- processors shall implement appropriate security measures to ensure personal data is secured;
- processors shall proactively notify breaches to operators without undue delay and ideally within a specified amount of time; and
- processors shall cooperate with the operators to provide information of the data breach and the evaluation of risks to players as a result of a breach.

6.6.5 The Obligation to Notify SAs

The GDPR considers three levels of risk i.e. 'low risk', 'risk', and 'high risk'. Notification requirements shall depend on the risk level of the personal data breach.

Operators are under an obligation to notify SA(s) without undue delay and in any event within 72 hours of becoming aware of a personal data breach. Notification is not required however, where the personal data breach is "unlikely to result in a risk to the rights and freedoms of natural persons".

Operators will therefore need to consider carefully whether this threshold is met by conducting a risk assessment to check:

- if specific factors present high risks (e.g. the data contains login details, passwords, bank account details);
- the volume of the breached personal data for the same player;
- the ease of identification of the affected data subjects from the personal data breached;
- whether the breach would cause any adverse effects for the players;
- how likely it is that adverse effects will materialise;
- whether the affected players will be able to overcome the adverse effects with minimal or limited difficulty;
- whether the breached data was already publicly available before the breach or can be easily accessed through publicly available resources;
- whether the information has been disclosed to third parties; and
- whether the intent of the breach was malicious.

If the operators have a main establishment in the EU and the personal data involved concerns cross-border processing, then it should notify its lead SA. The notification to SAs shall include:

- the nature of the personal data breach and a brief description of the incident;
- the categories and approximate number of players affected, and personal data records concerned;
- the name and contact details of the DPO from whom more information can be obtained;
- the likely consequences of the personal data breach; and
- the measures taken, or proposed to be taken, by the operator to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Operators should follow the process for reporting set out by the relevant SA. Where SAs have developed their own breach notification forms, operators should use these when notifying SA of breaches to ensure that all required information is provided.

Operators should also consider whether the data breach may trigger notification obligations to regulatory gambling authorities.

6.6.6 **The Obligation to Notify Players**

Operators must communicate to players, in plain language and in a simple manner, the existence of personal data breaches when it is likely to result in a “high risk” to their rights and freedoms. The communication shall include information regarding:

- the nature of the breach;
- a description of the likely consequences;
- the measures that the operator has taken, or plans to take, to address and mitigate the breach;

- if possible, the operator should also provide practical advice to players on how to protect themselves from the consequences; and
- the name and contact details of the DPO from whom more information can be obtained.

Operators will contact players individually directly by email, SMS or any other possible means. If such communication would involve a disproportionate effort, public communication should be used. The message should be accessible in alternative formats and relevant languages and, where feasible, further information and recent updates related to information provided in the notification (for example, if later on operator discovers that more data was breached than initially communicated) should be available via the operators' websites (where it is not possible to send message directly to the data subject) or directly communicated to the affected players.

For the communication to players, guidance from SAs, the EDPB and other bodies, such as law enforcement agencies, should be taken into account.

6.6.7 Accountability and record-keeping requirements

Regardless of whether or not the personal data breaches need to be notified to the SA, operators shall keep a summary record of each personal data breach, which should enable the SA to verify compliance with the reporting and notification requirements under the GDPR. The records must include:

- a chronology of the events leading up to the loss of control of the personal data;
- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and/or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident; and
- the measures being taken to prevent repetition of the incident.

Where notification of a personal data breach to the relevant SAs has been made, such notification may be used as a record to satisfy the record-keeping requirement.

- **The operator shall have in place a documented data breach response plan for dealing with a security incident and the identification and handling of any personal data breach; the plan should include the requirements set out in section 6.6.2 and following.**
- **The operator shall ensure that agreements with data processors define the processors' obligations on, among others, breach notification obligation, providing information to support breach identification and resolution.**
- **In the event of a personal data breach, the operator shall conduct a risk assessment to assess if the data breach needs to be notified to the relevant Supervisory Authority. When the SA needs to be notified, the operator should use, when existing, the SAs breach notification forms.**
- **The operator shall communicate to players the existence of personal data breaches when it is likely to result in a "high risk" to their rights and freedoms.**

The communication shall be done by any possible means and shall include the information contained in section 6.6.6.

- The operator shall keep records of each personal data breach, subject to internal data retention policies.

7. PRIVACY BY DESIGN AND BY DEFAULT

The GDPR has formalised the concepts of privacy by design and by default, requiring controllers to implement effective technical and organisational measures to ensure that the necessary safeguards (including security) and data protection principles are built into processes from the original concept stage and throughout the processing lifecycle.

This means that any action an operator undertakes that involves processing personal data must be done with data protection and privacy in mind, at every step, beginning with the initial design phase. Operators will be expected to undertake and demonstrate privacy by design when, by way of example:

- building new IT systems to process or access personal data;
- developing new internal policies or strategies with privacy implications;
- collaborating with an external party in a way that involves data sharing; or
- using existing data for new purposes.

Example

An operator wants to revamp its player account functionality. As part of ensuring privacy by design and default it should consider incorporating choices and controls for players in relation to their personal data processing, for example, making it easy to understand and amend their privacy settings.

Operators can ensure privacy by design and default through the following:

- Governance – leading from the top to develop a culture of awareness.
- Data protection risk management – identifying risks before they happen and establishing suitable controls.
- Having documented policies and procedures written in plain language to guide staff in how they need to handle the personal data they work with.
- Providing staff training and having performance management procedures.
- Documenting security standards that must be adopted across the business (including consideration of anonymisation or pseudonymisation of personal data).
- Having mandatory controls around the appointment of processors who have access to personal data.
- A robust DPIA process.

- **The operator shall document how it will implement privacy by design and default in the organization within its privacy by design and default methodology.**

8. PROCESSING REQUIRING DATA PROTECTION IMPACT ASSESSMENTS

The GDPR introduces a new obligation to do a DPIA before carrying out types of processing activities likely to result in high risk for individuals' interests.

8.1 When a DPIA is Required

An operator must undertake a DPIA before beginning any type of processing which is "*likely to result in a high risk*" for players. This means that, although the actual level of risk has not been assessed yet, the operator should screen for factors that point to the potential for serious impact on players.

Operators must follow the guidance of the competent SAs and of the EDPB relating to types of processing triggering a DPIA or not requiring a DPIA⁴. The GDPR provides a non-exhaustive list of conditions that trigger a mandatory requirement to conduct a DPIA. For example, an operator should carry out a DPIA if it engages in any of the following data processing activities:

- Solely automated decision-making, if the decisions are not based on human intervention and could produce legal effects or similarly significantly affect the players.
- Large-scale data processing, taking into consideration in order to determine the 'large scale' element: the number of players concerned, the volume of data and/or the range of different data items being processed and the duration of the data processing activity.
- Matching or combining data sets (e.g. data originating from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the player).
- Innovative uses or applications of new technological or organizational solutions to the processing of personal data (e.g. developing or implementing a new software or tool which involves processing of significant personal data or processing of personal data that exceed the reasonable expectations of the player). Each operator should define the meaning of '*new*' in their own context.

8.2 Conducting a DPIA

There is no specific form which must be used for DPIAs but many SAs provide suggested templates.

The purpose of undertaking the DPIA should first be to identify any potential risks to players' personal data. For each risk identified (e.g. unauthorised access, loss of personal data, repurposing etc.), whether new or existing, an operator should take account of the threat source and estimate the risk's likelihood and severity for the players.

Once the potential risks have been identified, the operator can proceed in the DPIA to determine and implement measures to appropriately manage those risks. For example, this may involve deciding against proceeding with an activity that gives rise to the risk, removing the source of the risk, changing the likelihood and/or consequences of the risk, finding alternative ways of processing, implementing remediation measures, accepting the risk, etc.

⁴ For this purpose, the EDPB makes publicly available the opinions on each SA list of processing requiring a DPIA. They can be found at https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

In accordance with Article 35, GDPR, the operator is obliged to seek the advice of the DPO when conducting any DPIA. This advice and the decisions taken should be documented as a part of the DPIA process. The operator will also need to ensure that DPIAs are kept under review at regular intervals.

- The operator shall undertake a DPIA before beginning any type of processing which is “likely to result in a high risk” for players.
- The operator shall document its methodology for conducting DPIAs, which shall include reviews at regular intervals.
- The operator shall seek the advice of the DPO when conducting a DPIA. The advice and the decisions taken should be documented in the DPIA process.

9. **SUPERVISORY AUTHORITY REQUEST HANDLING PROCEDURE**

This section provides guidance on defining the authority and scope of SAs in identifying for operators the relevant SA, as well as providing details on how to respond to relevant SAs.

9.1 **What is an SA?**

An SA is an independent public authority that supervises, through investigative and corrective powers, the application of data protection law inside the EEA⁵. Chapter 6, GDPR clearly states that each Member State shall provide for one or more independent public authorities (SAs) to be responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. A list is included at the end of this Code for reference in Annex B.

9.2 **Identifying a ‘Lead’ SA**

A lead SA is the authority with the primary responsibility for dealing with a cross-border data processing activity and will coordinate any investigation involving other concerned SAs. Identifying a lead SA is a key issue for operators who provide cross-border online gambling services across different jurisdictions. Cross-border processing has been defined as processing which takes place in the context of:

- establishments in more than one EU Member State if the operator is established in more than one EU Member State; or
- a single establishment of an operator in the EU but which substantially affects or is likely to substantially affect data subjects in more than one EU Member State⁶.

Identifying the lead SA depends on determining the location of the operator’s ‘main establishment’ or ‘single establishment’ in the EU. For operators with a main establishment in the EU, or which have appointed a representative in the EU, the relevant SA in that country will serve as the lead SA.

The main establishment can be determined as either the place of the operator’s central administration in the EU, or else the place where decisions on the purposes and means of the processing of personal data are taken. In the latter case, the establishment must have the

⁵ A list of all the SAs can be found at [https://edpb.europa.eu/about-edpb/board/members_en_and_in Annex B of this Code](https://edpb.europa.eu/about-edpb/board/members_en_and_in_Annex_B_of_this_Code).

⁶ Art. 29 Working Party, Guidelines for identifying a controller or processor’s lead supervisory authority as taken from Art. 4(23) of the GDPR.

power to have such decisions implemented in order to be able to be considered as the main establishment.

There may be cases where in addition to the place of central administration, another establishment makes autonomous decisions concerning the purposes and means of processing of personal data. This means that there can be situations where more than one lead SA can be identified, for example, in cases where a multinational company decides to have separate decision-making centres, in different countries, for different processing activities. In such cases, licensees must identify the processing operations falling under the respective remits of the two Lead SAs, in order to still benefit from the one-stop-shop mechanism.

There are borderline cases where operators will not always have a main establishment in the EU since this will depend on whether it meets the requirement for this as set out in the EDPB guidance. In these circumstances, the operator should designate the establishment that has the authority to implement decisions about the processing activity and to take liability for the processing, including having sufficient assets, as its main establishment. If the operator does not designate a main establishment in this way, it will not be possible to designate a lead authority.

To comply with the accountability principle, operators shall document its identification of the lead SA if any, and its reasoning for this. The GDPR prohibits “forum shopping”, therefore the operator must be able to demonstrate to the lead SA where decisions about data processing are actually taken and implemented.

If a lead SA is identified, it shall be informed by the operator, in order to make the communications between the operator and the lead SA easier and more transparent. On request, the process to identify the lead SA shall also be shared with any relevant authority.

9.3 Responding to an SA

Before responding to SAs it is important to know what the legal obligations are for operators. These obligations include, but are not limited to, making available an operator’s data processing records; notifying the SA about personal data breaches; where a residual high risk remains following DPIAs, carrying out consultations with a SA; communicating notification of appointment or change of DPO and changes to binding corporate rules and relevant certification.

- **The operator shall designate its main establishment and document the identification of its lead SA. The SA should be informed by the operator on its identification.**

III. CASE STUDIES

Case Study One: VIPs

An operator is setting up a VIP ('very important person/player') scheme for its most loyal players. This will include providing access for such players to a dedicated account manager, events, prizes, rewards and additional bonuses.

The operator will need to think through these specific issues in particular:

- 1) **Profiling:** the operator is likely to undertake profiling of players in order to identify those that are suitable for qualification for its new VIP scheme. The operator will be likely to want to rely on legitimate interests as its lawful basis for such profiling and must carry out a legitimate interests impact assessment to assess the balance between its business interests in setting up the scheme and selecting VIPs and the privacy rights of such players.
- 2) **Special Category Data and Proportionality:** given the relationship that VIPs may have with operator account managers, the operator needs to be aware that such players may openly provide more personal data to the operator than its other players. For example, VIPs may talk about their ethnicity, religion, family circumstances or perhaps mention that they will be in hospital the following month or provide other special category data. However, the operator shall ensure that, before processing special category data, it has the right legal basis to do so, therefore the operator needs to ensure that VIP account managers receive additional privacy training since such additional processing requires particular care and sensitivity.
- 3) **Security:** given the additional personal data that the operator is likely to be holding about VIPs and the expectation of such players that their account manager may have such information in the context of the relationship, the operator needs to take extra care to protect VIP data. This should include ensuring that there are robust access controls in place to limit the account managers and individuals who have access to additional data held about the player.
- 4) **Data Protection Impact Assessments:** given the scope of personal data processing and the possible processing of special category data, a risk assessment may be required for a VIP scheme, and where indicated a DPIA.

Case Study Two: Problem Gambling

An operator is subject to licence conditions and regulatory requirements that means it must take active steps to both identify patterns of potential problem gambling and to ensure that it has a robustly managed self-exclusion programme in place to protect players. The operator understands the importance of such initiatives but is concerned about the privacy considerations given that most gambling regulators rarely⁷ explain exactly what is expected and proportionate in terms of data processing. The reality is that it should be possible for the operator to balance both interests and protections provided the following steps are followed:

- 1) **Special Category Data and Lawful Basis:** in most cases, problem gambling information and, in particular, self-exclusion information does not involve or require the processing of

⁷ The exception is the Malta Gaming Authority which issued guidelines for operators in conjunction with the Maltese Data Protection Commissioner in May 2018 and which expressly mentions problem gambling data processing.

special category data and therefore the operator will do best to construct its programmes so they do not process special category data. It should not be necessary, for example, for the operator to have access to any medical records or health information regarding addiction in order to run its self-exclusion programme. The lawful basis for processing will therefore generally be: (i) compliance with a legal requirement (if the operator's jurisdiction has sufficiently clear laws or licence conditions on such processing requirements); (ii) public interest; and/or (iii) legitimate interests where (i) and (ii) do not apply. However, the operator must ensure that, if it does come into possession of special category data of players – for example, if a player were to choose to communicate with the operator providing details of health or addiction problems, then the operator will need to also have a lawful basis under Article 9, GDPR. This will need to be considered on a case by case basis and consideration of individual jurisdictional requirements, for example, some jurisdictions have local law derogations for processing such data to protect vulnerable individuals.

- 2) **Purpose limitation:** even though personal data may not be special category data for the purposes of GDPR, it is clear that a player's pattern of stakes, indicators of potential problem gambling activity or self-exclusion status is information that is nonetheless sensitive and private to players. The operator must therefore ensure that its systems allow for role-based access control, pseudonymisation and encryption.
- 3) **Data sharing:** in some circumstances it may be necessary for the operator to share problem gambling information with third parties, for example, with sports bodies or gambling regulators. Sharing should only be done where it is necessary and proportionate and information could not be otherwise disclosed in another form, such as anonymised or at least pseudonymised. A lawful basis is required for any disclosure and will usually exist where there is a legal requirement, it is needed to protect the vital interests of the individual or vulnerable persons (depending on jurisdiction specific public interest exemptions), or otherwise where a robust legitimate interests impact assessment and data sharing arrangement is in place. In addition, there is a trend of regulators to impose on operators broad and extensive obligations regarding high risk players and the requirements such as to consider to share AML, RG, and fraud checks between operators. All these measures require operators to take preventative steps and analyse a broad scope of players' data/activity to detect problematic behaviour at an early stage. Due to that approach operators must seek services from innovative service providers and use sophisticated tools in data analytics. Many of these are based on big data analytics and tracking/analysing players' data/activities from different sources (public ones, other operators, other companies, etc.). Therefore, it is important to recognize these new trends when analysing players' behaviour.
- 4) **Automated decision-making:** the need to protect players from problem gambling means that the operator may consider developing or improving technologies to help identify and flag potentially vulnerable patterns of behaviour or individuals. Given the data and player volumes at stake, automated processing technologies are often the most appropriate way to manage such potential risks and complex datasets. The operator has two options here:
 - a. Ensure that such technologies only ever provide a 'first pass' indicator for account teams so that any decision to actually stop, suspend or close an account which may have a significant effect on a player are always subject to meaningful human involvement (this is considered not to be solely automated decision-making).
 - b. Ensure that applicable Member State law allow for the solely automated decision-making by analysis of the relevant public interest or other derogations. In these cases, it is not feasible to obtain the consent, since such consent would not be freely given and capable of being withdrawn.
 - c. If carrying out solely automated decision-making, the operator will also need to ensure they are able to give players a means to contest the decision, and to request human involvement.
- 5) **Data protection impact assessments:** the operator should undertake a risk assessment, and where indicated a DPIA, in respect of any problem gambling programme and, given changes in guidance, technologies and gambling regulatory requirements, this should be revisited and revised regularly. The operator should consider in the context of such

assessments, consultation with relevant stakeholders to consider different viewpoints and to be able to better improve systems and safeguards with a privacy by design and default approach.

Case Study Three: Direct Marketing

An operator is looking to revamp its direct marketing programme to expand the services that are marketed to its players. To ensure that privacy rights are protected, however, operators need to consider several key issues:

- 1) **Clarity and Transparency:** the operator may have various brands and may also be within a group with different legal entities operating different ones. The fact that operators operate different brands via a different group of companies does not mean that from a data privacy perspective all these companies must be data controllers. We can have one or few selected entities responsible for the processing of personal data on the group level. In the situation where we have one controller for different brands owned by different companies, the data controller can send marketing messages about all brands to the whole customer database (no need for group consent), as long as the customers are aware that they will receive marketing from all respective brands and that each message contains an unsubscribe option. Therefore, it is very important that in constructing any direct marketing, the operator makes the consent mechanisms and preference centres easy and understandable to players: will they be only receiving marketing about the same brand they have signed up to already or multiple brands from the same entity? Similarly, when individuals choose to unsubscribe, is it clear what they will still receive and what they will not? It can be helpful to design several options and then engage with players or user groups to understand what works best and is clearest in practice.
- 2) **Self-exclusion:** the rights of players in respect of self-exclusion will always trump any legitimate interests of the operator in respect of direct marketing. Self-exclusion status should immediately put a stop on any direct marketing activity.
- 3) **Profiling:** most modern direct marketing techniques involve some manner of profiling by creating specific audiences and segments to make marketing relevant and targeted. When using profiling, the operator must ensure:
 - a. Its players understand the profiling and how their personal data is used in order to create such profiles;
 - b. if relying on legitimate interests as the lawful basis for such activity, players must have a right to object and this must be brought to their attention;
 - c. proportionality in the processing and that assessments are conducted to ensure that individual rights are balanced against marketing drivers.
- 4) **Local legislation:** GDPR contains the high-level obligations around processing of personal data but the specific rules on direct marketing by electronic means are set out in local legislation and can vary. The operator must therefore consider carefully which laws apply and whether it can have a one size fits all approach or needs to have different approaches for different territories.
- 5) **Purpose creep:** The operator is hoping to expand its direct marketing activities, but it needs to bear in mind the consents it has already obtained from players. It won't be possible to just expand out marketing to cover multiple non-similar services if consent was originally only obtained for one. If the nature of processing is going to change then the operator will need to consider either programmes for obtaining new updated consents or just implementing its new consents and marketing for new players who are presented with it.

- 6) **Inactive players:** Although players shall always receive service communication, even when in inactive status, as part of the services, for marketing communication the answer is not that straightforward. Given the nature of inactive status, operators should make it clear in their policies how they will send marketing to inactive players. For example, operators can determine that they will send marketing communication to the inactive players that are inactive up to four years.

Case Study Four: Fraud Detection

Measures to prevent fraud are essential to an operator in order to protect its business and comply with applicable laws. However, the operator knows that this should not mean the fettering of privacy rights. Key issues for the operator to consider to keep this balance are as follows:

- 1) **Lawful basis:** some processes the operator must follow may be dictated by clear legal requirements (for example, in the case of know your customer checks). In most cases however, fraud detection techniques and technologies are not directly specified under regulation, meaning the operator will need to identify another lawful basis for the processing. Legitimate interests is generally the most appropriate lawful basis in such cases, but the operator must carry out a robust legitimate interests impact assessment first, paying close attention in particular, to issues around data minimisation and proportionality.
- 2) **Vendors:** the operator may be looking to rely on third parties to assist with its fraud detection initiatives, whether by licensing technology or using third party expertise and additional data sets. The operator must ensure that it carefully considers whether such vendors are acting as a separate controller or as a processor depending on the activities that such vendor is carrying out and the control they have. Appropriate contractual protections must then be put in place. However, it is not enough just to rely on contractual provisions and the potential for enforcement. The operator must carry out assessments in deciding on which vendor to use, record such assessment and ensure that these are kept up to date, as services change and may become subject to renewal reviews.
- 3) **Automated decision-making:** as with problem gambling above, the operator must consider whether any automated processing conducted for fraud detection constitutes automated decision making. Will there be any consequence which has a legal or similarly significant impact on the player, or can meaningful human involvement be incorporated into the process?
- 4) **Accuracy:** inaccurate data can be a cause of indications of fraud and so the operator must ensure that safeguards are in place to ensure data is collected accurately and can easily be corrected where errors are identified.

Case study five: Affiliates

One of the very common ways of cooperation in this industry is affiliate marketing. Affiliate providers are independent parties that hold websites with high number of visits/traffic. Due to that fact, operators have an interest to advertise their products/services on the affiliate website. In return the affiliate is paid for a player that came from its website to operators. There are different types of

arrangements with affiliates, and from the type or arrangements and their role depends the nature of processing which they carry out:

- 1) **Fixed fee:** Where the affiliate is getting a fixed fee for advertising an operator and redirecting traffic to its website, there are no data privacy implications since parties are not sharing any data, and each party is solely responsible for its data privacy compliance.
- 2) **Fee per revenue/customer:** In this situation a fee is paid per number of customers redirected, or revenue generated or some other metrics that is related to the specific player redirected thanks to affiliate activity. In this case affiliates most likely will not need personal data of players, but they do need to get information about the number of players or revenue generated, in order to verify payment of their fee. For these purposes, operators should share fully anonymised data or pseudonymized up to that level that identification of data subjects is impossible. In most cases the best way to achieve this is by using tracking via cookies, that use pseudonymised data and in that way operators would ensure that they are not sharing personal data. If used by operators these cookies should not require consent. In this scenario the affiliate and the operator are independent controllers where each is solely responsible for its processing operations, and they will not share personal data for the purpose of this cooperation.
- 3) **Advertising third party products/services:** In this case the operator can pay the affiliate to send its marketing material, to affiliate customers. Both parties are independent controllers responsible on their own for their processing operations. This means that the affiliate will have to make sure that it has consent from its customers to advertise third party products/services.

IV. CONDITIONS OF ADHERENCE

By declaring its adherence to the Code, the operator commits to comply with its requirements. Operators shall declare that they will comply with all parts of the Code and cannot declare to adhere only to a certain part of the Code or to not apply certain sections of the Code.

The operators that have declared adherence to the Code commit to submit to the chapter 5 on “Governance”. If an operator fails to meet the minimum requirements of the Code, it will be subject to the enforcement mechanisms as set out in the section below named “complaints”.

Adhering to the Code does not ensure automatic protection against possible interventions or actions by the competent SAs (or other authorities) in the course of their supervision and enforcement activities. Complying with the requirements of the Code will help adhering operators demonstrate that they are accountable with regard to data protection rules, which will have a positive impact in the context of supervision and enforcement activities.

The Code was drafted to be fully consistent with the GDPR. Its application by any operator should not result in any conflict with its internal policies, procedures or standards. Any such conflict must be resolved before declaring adherence to the Code: operators should ensure that their legal or contractual obligations do not contradict any part of the Code before declaring their adherence to its terms. In case of changes in EU data protection law, or any law that would impact the content of the Code, an operator willing to adhere to the Code is required to comply with the new legislation, even if such legislation has not been implemented yet in the Code and even if this would entail new or conflicting obligations regarding the Code. Furthermore, a declaration of adherence to the Code does not negate any operator from having to comply with the GDPR and/or applicable Union or Member State data protection law. In the case in which a Member State has stricter rules regarding data protection, such national provisions shall take prevalence on the Code.

a) **Procedure to declare adherence**

Operators shall submit their declaration of adherence to the Monitoring Body⁸, following the declaration form contained in Annex 1 of the Code. The Code Secretariat will publish and maintain an updated version of the declaration of adherence in the Code register.

The Monitoring Body, in consultation with the Executive Board, will establish procedures and guidelines to assess and review the member’s declarations of adherence. These guidelines shall (i) provide for a more stringent approach in case of a declaration supported by self-assessment and (ii) explain that certifications eligible for certification-based adherence must be sector-specific and cover not only the security, but also all the personal data protection principles as defined in the EU legal framework.

The declaration of adherence shall be supported by at least either of the following:

- Self-assessment by the operator; or
- Certification(s) by independent third-party auditors.

When completing the self-assessment of compliance, the operator shall confirm that its processing of personal data fully complies with the requirements set out in the Code. The Monitoring Body, upon receiving the declaration of adherence by the operator, shall verify the operator’s compliance with the Code through a plausibility check.

Alternatively, the operator can support its compliance with the Code by independent third-party certificates and audits that the operator has undergone with regard to data processing and

⁸ Or to the Executive Board, until a Monitoring Body is appointed.

security requirements. Any such third-party certificates and audits that were considered to be relevant by the Monitoring Body shall be cited in the report of the approval by the Monitoring Body.

The Monitoring Body shall review the declaration of adherence, but may not exceed 30 working days counting from the date the Monitoring Body receives all relevant information. If the declaration of adherence is not complete, the Monitoring Body may request the operator to provide any missing document or information required to complete its declaration of adherence.

When the Monitoring Body deems the operator's compliance with the Code to be satisfactory, it shall approve the declaration of adherence. Once approved, the Code Secretariat will notify the operator of its acceptance and will incorporate the declaration of adherence into the Code register within 10 working days.

The Code register shall at least provide the following information:

- Name of the member adherent to the Code;
- Date of declaration of adherence approval;
- Report of the declaration of adherence approval by the Monitoring Body;
- Due date of the declaration of adherence.

After publication in the Code register, the member may apply any compliance mark made available for this purpose to its website and to relevant communications and publications, under the terms and conditions as set by the General Assembly.

b) Procedure to review the adherence to the Code

The compliance of any member that has declared its adherence to the Code will be monitored by the Monitoring Body, as noted above.

Any declaration of adherence shall be reviewed every twelve months unless any significant changes occur to the declaration of adherence itself, in which case they shall be reviewed earlier. Each individual annual revision does not need to cover all provisions of the Code; however, over successive reviews, all provisions of the Code will be covered.

If the Monitoring Body becomes aware of any non-compliance of a member, the Monitoring Body can request the member to take specific measures to make that operator comply with the Code.

In the event that a declaration of adherence is revoked, the Code Secretariat shall delete that particular member from the Code register. In this case, the operator shall cease to make reference to the Code in any of its documentation or publications, including its website.

c) Complaints

- Complaints of operators against decisions of the Monitoring Body An operator whose declaration of adherence has been rejected by the Monitoring Body may submit a revised request of declaration of adherence or file a complaint.
- Complaints of players against any member's compliance with the Code In the case of a complaint regarding a member's compliance with the requirements of this Code, the player is encouraged to contact the member first in order to obtain a satisfactory solution.

If no such solution can be found, the player can submit a complaint to the Monitoring Body that reviewed and approved the respective declaration of adherence.

The Monitoring Body shall review the complaint, require the member to provide any relevant information for the purposes of fact finding and initiate a complaint handling process.

d) **Compliance Mark**

The Executive Board will develop a compliance mark to be used as a public-facing symbol of a member's adherence to the Code Requirements ("Compliance Mark"). The Compliance Mark will be approved by the General Assembly.

Any member that has been duly registered in the Code register is entitled to use the applicable Compliance Mark.

Should a dispute concerning non-compliance arise, a member is entitled to continue using the Compliance Mark. After receiving a final decision to revoke the declaration of adherence, that member must immediately cease to use the Compliance Mark.

Explanatory chart of process to adhere to the Code



V. GOVERNANCE OF THE CODE

This chapter describes how the Code is managed, applied, and revised, including the roles and obligations of its governing bodies.

The Code Governance Bodies are tasked with the implementation and administration of the Code.

a) **General Assembly**

a.1) **Composition**

The General Assembly is composed of the founding operators – bet365, Betsson Group, GVC Holdings PLC, Kindred Group, William Hill Plc – and all other operators, whose applications to join the Code have been approved by the General Assembly.

Each member of the General Assembly has one vote and may be represented by one or more individuals with expertise in the online gambling sector and data protection law.

Each member shall inform the Chairman of the General Assembly, prior to each General Assembly, of who their representatives are.

A member may cease to participate to the General Assembly, by giving the Chairman of the General Assembly 12 months prior notice and promptly paying membership fees during that period. If a member fails to comply with the 12 months prior notice period (for whatever reason, including exclusion), that member shall pay the membership fees applicable to the remainder of the 12 months' notice period.

a.2) **Powers**

The General Assembly shall have the following powers:

- designate the Chairman of the General Assembly and the members of the Executive Board;
- approve the Monitoring Body accounts;
- approve annual membership fees and any other fees as proposed by the Executive Board;
- approve new members;
- decide on action or sanctions to be applied by the Monitoring Body, e.g. the suspension or exclusion of any member, following a proposal by the Monitoring Body;
- approve changes to the Code, based on proposals of the Executive Board;
- decide on any other matters as requested by the Executive Board.

a.3) **Chairman of the General Assembly**

The Chairman of the General Assembly shall be elected by the General Assembly meeting for a term of two years, with the possibility of renewing its mandate for any number of successive additional two-year terms.

a.4) **Meeting**

The Chairman shall convene the General Assembly at least once a year, in the first quarter of each year, to approve at least the Monitoring Body's accounts and annual fees, and to appoint the Chairman of the General Assembly and the members of the Executive Board, whenever applicable. The Chairman shall also convene a General Assembly, upon request of at least two members of the General Assembly or of the Monitoring Body, which have to clearly state in writing the matters of the agenda and the purpose of the meeting.

The members may participate in a General Assembly either physically or remotely via electronic meetings or by conference calls.

a.5) Quorum and majorities

The General Assembly's decisions shall be considered validly taken only with a majority of the votes of the members of the General Assembly. However, if there is not a quorum present when a meeting is first called, a simple majority of those present or represented at an adjourned meeting will suffice to approve the decision.

b) Executive Board

b.1) Composition

Unless otherwise agreed by a decision of the General Assembly, the Executive Board shall be comprised of a maximum of 10 members.

Each member of the Executive Board is entitled to one vote and may appoint up to two individual named persons to represent them at the Executive Board, and who may name a substitute if they are unable to participate in an Executive Board meeting. Individuals who represent their organisations in the Executive Board shall have a proven expertise in the online gambling sector and/or data protection.

The Executive Board may pass a resolution to invite interested third parties to join an Executive Board meeting with a view of strengthening the balanced representation of stakeholders interested in participating in the Code, from both the private and public sectors.

b.2) Powers

The Executive Board shall have the following powers:

- monitor changes in European Union data protection laws and propose changes to the Code for approval by the General Assembly;
- in consultation with the Monitoring Body, define and propose the content of the Code declaration of adherence and any guidelines for self-assessment;
- in consultation with the Monitoring Body, define and propose minimum requirements for the assessment of those declarations of adherence by the Monitoring Body;
- define and propose guidelines for Code certification by auditors, specifically in order to identify appropriate existing standards and certification schemes that can be used to confirm compliance with all, or parts, of the Code. Within such guidelines, the Executive Board will endeavour to take advantage, when appropriate, of existing third-party standards, schemes and audits which are relevant to (certain parts of) the Code;
- define and propose more detailed guidelines for the application and interpretation of the Code;
- adopt Compliance Marks that may be used by members;
- approve the Monitoring Body;

- approve the Code Secretariat;
- approve any external third-party auditors;
- discuss and submit for the approval of the General Assembly, membership fees and, in consultation with the approved Monitoring Body, fees for declaration of adherences and their reviews, complaints fees, and any other fee that might be applicable;
- propose, in consultation with the Monitoring Body, for the approval of the General Assembly, the allocation of a share of the annual membership fees, from members that have signed a declaration of adherence, to safeguard the Monitoring Body's legal minimum functionality and independence;
- propose, in consultation with the Monitoring Body, the appropriate actions and sanctions that the Monitoring Body can apply in case of an infringement of the Code or in case a member is not providing the information necessary to review a possible infringement of the Code to the Monitoring Body;
- work on particular issues and new developments impacting the Code, where necessary by establishing and proposing an annual work programme in consultation with the SAs, the EDPB and European Commission and, where necessary, by developing proposals for the improvement of the governance.

b.3) **Board**

The Executive Board shall elect a Chairman from amongst its members, for a period of two years, with the possibility of renewing their mandate for any number of successive additional two-year terms.

b.4) **Meeting**

The Chairman shall convene the Executive Board at least two times a year. The Chairman shall also convene a meeting, upon request of at least two members of the Executive Board, who have to clearly state in writing the matters of the agenda and the purpose of the meeting.

The Members may participate in the Executive Board either physically or remotely via electronic meetings or conference calls.

Provided that copies of all relevant documents are first sent to all the members of the Executive Board, a resolution of the Executive Board may also be taken without a meeting if it is agreed, in writing, by all members of the Executive Board.

b.5) **Quorum and majorities**

The quorum for all meetings, at first call, of the Executive Board shall be a simple majority of votes of all the members of the Executive Board. If a meeting is not quorate, it shall be adjourned to a date at least one day after the date of the first meeting. The quorum for a meeting adjourned shall be a simple majority of the members of the Executive Board present or represented.

b.6) **Disputes**

The Executive Board shall develop appropriate policies to assure that interests are disclosed, and conflicts are avoided. Mechanisms will include separation of duties, recusal or other policies undertaken by the Executive Board, and possibilities for the General Assembly to raise objections against individual Executive Board members.

c) **Monitoring Body**

The Monitoring Body, accredited in accordance with Art. 41 GDPR shall perform the following functions:

- review and approve declarations of adherence by operators;
- regularly monitor whether the operations of the members are in accordance with the Code;
- review and handle complaints about infringements of the Code;
- establish procedures and structures to deal with complaints about infringements of the Code;
- implement procedures and structures that prevent conflicts of interests;
- take appropriate action against a member in case of an infringement of the Code;
- inform the competent SA of final actions taken against members and the reasons for taking them.

A Monitoring Body, which was already approved as Code Monitoring Body by the Executive Board before obtaining an accreditation from the competent SA, will be obliged to apply for an accreditation pursuant to Art. 41 GDPR within a reasonable timeframe. In case the accreditation decision is not made within reasonable time or the accreditation is finally rejected, the Executive Board shall suspend or revoke the approval of the body. If this situation arises, any member that was approved by the suspended or revoked Monitoring Body will have their declarations of adherence reviewed by the Executive Board. The Monitoring Body is allowed to use the information obtained during a review process only for purposes related to its responsibilities pursuant to the Code. The Monitoring Body, including any persons working on its behalf, is bound by an obligation of confidentiality, and ensures that all information received in the context of its activities shall be kept undisclosed and adequately protected from unauthorized access and shall be deleted when no longer necessary for the purpose it was obtained, unless otherwise determined by applicable mandatory law.

Any decision or action taken by the Monitoring Body shall be documented. Such documentation shall include, at least, the decision or action, date, substantial and essential circumstances in which such decisions or actions were based, main reasoning and individuals responsible. This documentation shall be kept at least for three years.

Upon reasonable request of the Monitoring Body and in accordance with its duties and competencies under the Code, members are under the obligation to cooperate with the Monitoring Body with respect to providing information to the Monitoring Body. Breach of such an obligation could amount to an infringement of the Code.

d) **Code Secretariat**

The Code Secretariat performs the following functions:

- Maintain a public register of declarations of adherence by members;
- Maintain a public register of certificates;
- Maintain a public register of Code guidelines;
- At the request of the Chairman of the General Assembly, convene General Assembly meetings, prepare General Assembly meetings and draft minutes of the meetings;
- At the request of the Chairman of the Executive Board, convene Executive Board meetings, prepare meetings and draft minutes of the Executive Board;

- Promote the Code in Member States;
- Maintain the Code website;
- Perform other related functions at the request of the Executive Board.

e) **Review of the Code**

When appropriate, and in any event at least every three years, the Code and its guidelines shall be reviewed to reflect relevant legal and technological changes and best practices, as well as experiences in the practical application of the Code.

An additional review of the Code and its guidelines can be initiated at the request of at least two members of the Executive Board or the Monitoring Body.

Every change shall be first approved by the General Assembly, which shall then submit the revised Code for endorsement in accordance with Art. 40(5) GDPR. Comments from the SAs and the EDPB should be incorporated as appropriate, approved by the General Assembly and published.

f) **Finances**

f.1) **General**

The costs for the Secretariat and the Monitoring Body should be covered by fees raised by the members of the Code.

f.2) **Secretariat**

The General Assembly shall decide in the annual General Assembly meeting the adequate share of the membership fees to cover the Secretariat administration costs.

f.3) **Monitoring Body**

Fees that members pay to obtain the approval of a declaration of adherence shall be allocated to cover the operating costs of the Monitoring Body. The fees apply regardless of the outcome of the declaration of adherence process.

Additionally, the Monitoring Body shall receive an adequate share of members annual membership fees to safeguard the Monitoring Body's legal minimum functionality and independence, including its complaints mechanism and constant monitoring.

The Monitoring Body must present their financial records to the Executive Board until January of each year, which will then submit them to the approval of the General Assembly.

Complaints may be subject to fees, which shall be cost-based and approved by the General Assembly.

Annex A: Template Declaration of adherence

1) Identity of the operator

[Name, legal form, head office, place of registration]

2) Contact information of the operator's designated data protection officer(s) in charge of privacy matters

[Name, e-mail address]

3) Identity of Monitoring Body that verified this declaration of adherence

[Name, location, e-mail address]

4) Means of adherence

This declaration is supported by:

- Self-assessment by the operator.
- Certification by an independent third party.

5) Third party certifications (if any)

The operator has undergone the following certifications in the last 12 (twelve) months prior to submitting this declaration of adherence, and undergone re-certification (to be specified for each certification):

[Standard 1 against which compliance is assessed] – [Name of accrediting body, legal form, seat of establishment]

[Standard 2 against which compliance is assessed] – [Name of accrediting body, legal form, seat of establishment]

[...]

6) Signature of legal representative By signing below the operator confirms that:

- (a) as of the date of this Declaration the processing of data in the operator's company adheres to the Code Requirements;
- (b) the operator will comply with the complaints and enforcement procedures in Section IV, Conditions of adherence, of the Code.

[Operator's name]

By: _____

Name: _____

Title: _____

Date: _____

Annex B: List of concerned Supervisory Authorities

Österreichische Datenschutzbehörde	Austria
Autorité de la protection des données (APD-GBA)	Belgium
Commission for Personal Data Protection	Bulgaria
Croatian Personal Data Protection Agency	Croatia
Commissioner for Personal Data Protection	Cyprus
Office for Personal Data Protection	Czech Republic
Datatilsynet	Denmark
Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)	Estonia
Office of the Data Protection Ombudsman	Finland
Commission Nationale de l'Informatique et des Libertés – CNIL	France
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	Germany
Hellenic Data Protection Authority	Greece
Hungarian National Authority for Data Protection and Freedom of Information	Hungary
Data Protection Commission	Ireland
Garante per la protezione dei dati personali	Italy
Data State Inspectorate	Latvia
State Data Protection Inspectorate	Lithuania
Commission Nationale pour la Protection des Données	Luxembourg
Office of the Information and Data Protection Commissioner	Malta
Autoriteit Persoonsgegevens	Netherlands
Urząd Ochrony Danych Osobowych (Personal Data Protection Office)	Poland
Comissão Nacional de Protecção de Dados – CNPD	Portugal
The National Supervisory Authority for Personal Data Processing	Romania
Office for Personal Data Protection of the Slovak Republic	Slovakia
Information Commissioner of the Republic of Slovenia	Slovenia
Agencia Española de Protección de Datos (AEPD)	Spain
Datainspektionen	Sweden
The Information Commissioner's Office	United Kingdom

Persónuvernd

Data Protection Office, Principality of Liechtenstein

Datatilsynet

Data Protection and Information Commissioner of Switzerland

The Information Commissioner

Iceland

Liechtenstein

Norway

Switzerland

Isle of Man

Annex C: List of documents for the operators' compliance framework

In order to establish a compliance framework to demonstrate compliance with the principle of accountability and the Code requirements, here below is a non-exhaustive list of documents that may be used by operators:

- Data map(s)
- Record of processing
- Data protection policy
- Privacy policy
- Data retention policy
- Data subject consent form
- DPIA register
- Supplier data processing agreement
- Data breach response and notification procedure
- Data breach register
- DPO job description
- Standard Contractual Clauses for the Transfer of data to Controllers
- Standard Contractual Clauses for the Transfer of data to Processors
- Register of Privacy Notices
- Data Subject Access Request Procedure
- Data Protection Impact Assessment Methodology
- Cross Border data Transfer Procedure
- Documents regulation on security of data

DEFINITIONS

Any terminology used in this Code of Conduct which is defined in the [General Data Protection Regulation](#) (e.g. personal data, processing, controller, processor, etc.) shall have the meaning and interpretation as defined in accordance with Article 4, Regulation.

- '*confidentiality*' means that personal data can be accessed only by authorised people, only for a specific period of time and from systems that they are authorised to use.
- '*DPIA*' means a data protection impact assessment.
- '*LIA*' means a legitimate interests impact assessment.
- '*integrity*' means that personal data cannot be modified in an unauthorized or undetected manner.
- '*member*' is equal to the definition of '*operator*', but used only in the chapters "Conditions of Adherence" and "Governance" to distinguish the operator that had its declaration of adherence to the Code approved.
- '*necessary*' is a term that covers those situations where it is not reasonably possible to achieve the stated objective in a less intrusive way.
- '*online gambling service*' means any service which involves wagering a stake with monetary value in games of chance⁹, including those with an element of skill, such as lotteries, casino games, poker games and betting transactions that are provided by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services¹⁰.
- '*operator*' means any natural or any legal person providing an online gambling service and anyone acting in the name of or on behalf of such person¹¹. Unless stated otherwise, throughout the Code '*operator*' equals to 'controller' or 'data controller'.
- '*player*' means any natural person who holds a player account with the operator and participates in the online gambling service. Unless stated otherwise, throughout the Code '*player*' equals to 'individual' or 'data subject' or 'customer'¹².
- '*security incident*' means any potential breach of security which needs to be assessed by the operator to evaluate if a personal data breach has taken place.

⁹ This definition encompasses also the situation in which, to participate in a game of chance, no deposit is required from the player, e.g. free bets.

¹⁰ Ibid., Art. 3 (a).

¹¹ Commission Recommendation of 14 July 2014 on principles for the protection of consumers and players of online gambling services and for the prevention of minors from gambling online, Art. 3 (f).

¹² Ibid., Art. 3 (c).

EGBA | European Gaming &
Betting Association

Rue Gray 50
1040 Brussels, Belgium
EU Transparency register:
29508582413-52
www.egba.eu