MGA

The General Data Protection Regulation

Guidelines issued by the Malta Gaming Authority, in consultation with the Information and Data Protection Commissioner, for the Maltese Gaming Industry

Malta Gaming Authority

Contents

1 Scope

These guidelines are intended to provide B2C licensees with guidance on the processing of personal data carried out throughout the course of their gaming service operations.

These Guidelines have been developed after a consultation process with the Information and Data Protection Commissioner who ascertained that the provisions of these Guidelines comply with the General Data Protection Regulation. This notwithstanding, such guidelines and the interpretations contained herein are without prejudice to any decision which the Commissioner may take in relation to complaints and, or to any other specific data protection issue. These interpretations are also without prejudice to any further guidelines or opinions that might be issued by the Article 29 Data Protection Working Party and, as from 25 May 2018, by the European Data Protection Board.

These Guidelines are considered to be a living document and will be further developed over time as practical issues arise with the effective implementation of the GDPR.

These guidelines are to be read in parallel with legal requirements imposed on Operators by virtue of Maltese gaming laws, and are without prejudice to the said legislation. These guidelines are not intended to replace any law, legal obligation or decision.

2 Definitions

Personal data: means any information relating to an identified or identifiable natural person (in the following defined also as "data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number (e.g. client number), location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Special categories of personal data: means personal data disclosing racial or ethnic origin, religious or philosophical beliefs or trade-union membership, as well as genetic data, biometric data aimed at unequivocally identifying a natural person, data related to the health or sex life or sexual orientation of the person.

For the avoidance of any doubt, data pertaining to self-exclusions is not considered to be data related to health, and hence does not fall under special categories of personal data. In the event that, throughout the course of communication with a player, a B2C licensee is forwarded any specific medical data, such as a doctor's report, or information about a player's health, such information is to be treated as a special category of personal data and therefore the provisions and safeguards applicable to such data as laid down within the GDPR are to be adhered to.

Processing: means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring,

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data controller: means the entity which alone or jointly with others determines the purposes and means of the processing of personal data.

For the purposes of the GDPR, a B2C licence holder which determines the purposes and means of the processing of personal data is considered a data controller.

Data processor: means the entity (company or individual) processing personal data on behalf of the controller.

For example, a cloud service provider is considered a data processor processing data on behalf of the company (client) which determines the purposes and means of the processing of its customers' personal data.

3 Applicability

3.1 Territorial scope

From a territorial perspective, the GDPR does not differentiate between data controller and data processor and sets out the same territorial scope for both of them.

Mainly, the GDPR applies in the following two situations:

- the processing of personal data takes place in the context of the activities of an establishment (i.e. the effective and real exercise of activity through stable arrangements) of the controller or processor within the EU; or
- the processing of the data of individuals within the EU takes place by a controller or processor not established in the EU.

For the applicability of the GDPR, it is therefore not necessarily decisive where the data is being processed.

These guidelines apply to B2C licensees that process personal data during the course of their business activities of an establishment in Malta regardless of whether the actual processing takes place in the EU or otherwise.

Non-EU established companies will be subject to the GDPR where they process personal data about EU data subjects in connection with:

- the offering of goods or services" (payment is not required); or
- monitoring data subjects' behaviour within the EU (including online profiling activities, i.e. the tracking of individuals online to create profiles, including where this is used to take decisions to analyse/predict personal preferences, behaviours and attitudes).

While reference is made to data processors, such as cloud service providers and data centers, throughout the guidelines, this document is by no means sufficient to ensure their compliance with the GDPR, and it is advised that data processors seek further legal guidance on the matter.

3.2 Material scope

The GDPR applies to the processing of personal data wholly or partly by automated means (the latter meaning any processing where certain steps are carried out by individuals, such as entering data into a computer) and to the processing other than by automated means of personal data which is contained or intended to be contained in a filing system which are structured according to specific criteria.

The material scope is interpreted in a very broad manner in order to ensure a high level of protection, so basically the GDPR will become relevant for companies as soon as any processing of personal data takes place.

4 Lawful Processing of Personal

Under the GDPR, personal data can only be processed if, and to the extent that, at least one legal basis for the processing listed below applies:

a) the data subject has consented to the processing;
b) it is necessary for the entry into, or performance of, a contract with the data subject or in order to take steps at his request prior to the entry into a contract;
c) it is necessary for compliance with a legal obligation under EU law or national law;
d) it is necessary in order to protect the vital interests of the data subject or of another natural person;
e) it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and, or
f) it is necessary for the purposes of legitimate interests pursued by the data controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects.

These guidelines will focus on four particular bases, 'Legal obligation', 'Contract', 'Consent' and 'Legitimate Interest' since it is expected that, generally, most of the Operators' processing activities will be carried out relying on one or more of such bases. It is imperative that Operators determine the appropriate legal basis (or bases) from the start, since, as specified below, the legal basis on which the personal data is being processed must be communicated to the respective data subjects.

4.1 Legal Obligation

A legal obligation imposed on the Operator by virtue of gaming legislation, AML legislation, or any other specific law, may be determined as the appropriate basis on which to process players' personal data. References to such a basis are made throughout the document.

4.2 Contract

The contract entered into between a player and an Operator can serve as one of the legal basis on which a player's personal data is processed. However, the term 'necessary for the performance of a contract' needs to be interpreted strictly. Processing is deemed necessary if the contract could not be fulfilled without the processing taking place, therefore it is important to determine the scope of the contract or service, and to limit the personal data being processed to what is strictly necessary in order to provide the gaming service.

For example, processing personal data for marketing purposes cannot be considered to be strictly necessary to offer a gaming service and consequently such processing activity must rely on a separate consent which should be obtained in accordance with the requirements of the GDPR as explained below. If the player refuses to consent to this processing purpose, the operator may not deny services to the player, or apply any increased fees.

For example, online subscription forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the required fields (e.g. the player will not be able to receive special offers and promotions.

The contract itself, therefore, is not to include or to be merged with consent, when consent itself is being used as a legal basis for processing which is not necessary for the performance of the contract.

It must be noted that the player may exercise the right to restriction, rectification and access when the data processing is based on contract.

4.3 Consent

The more a controller relies on consent as a legal basis for the processing, the more the data subject is in control of their activities, and the greater the trust between the two. However, it must be kept in mind that consent may be withdrawn, and might hence not be an ideal basis for the processing of data in the course of specific activities pertaining to the gaming operation.

Consent must be freely given: players must specifically opt-in by checking boxes which are not pre-checked. Consent is not to be bundled up in non-negotiable terms and conditions, and is not to be presumed to be given. Additionally, each specific tick-box for consent should only cover processing activities which are carried out for the same purpose or purposes; multiple purposes must result in multiple, specific consents[1].

By way of a general example, in order for consent to be valid, separate consent must be sought from the players when the operator would like to send marketing via email, and when the operator would like to share the details of the player with other companies within the same group of companies or with third parties outside the group.

[1] Recital 32 GDPR.

If an Operator would like to process the data for a new purpose, then it would need to seek new consent from the player for the new processing purpose. The original consent will never legitimise further or new purposes for the processing[2].

Consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service. Therefore, as explained above, denial or withdrawal of consent for marketing purposes, may not result in the Operator denying services to the player, or in the Operator applying any increased fees[3].

In order to provide a summary, the data subject must be provided with the following information:

a) specific details on the operator which is seeking the consent, if the consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named (details of at least one data processor, such as cloud service providers and data centers, need not be provided, although Operators will need to make available a full list of recipients or categories of recipients including processors (please refer to section 5 - Right to be informed - below for more details);
b) the purpose of every processing activity for which consent is being sought;
c) the type of data that will be collected and used;
d) the existence of the right to withdraw consent, and how one may avail himself of this right (which in any case cannot be more burdensome than the manner in which one can give consent, e.g. via the same electronic interface, like a website or an app, used to opt-in);
e) information about the use of the data for decisions based solely on automated processing, including profiling (kindly refer to section 6 - Automated decision making and Profiling - below).

It must be noted that data processing based on a player's consent is subject to data portability (kindly refer to section 5 - Right to Data Portability - for more information), and the player may exercise the right to erasure, restriction, rectification and access.

If an Operator finds that the consent obtained under previous legislation will not meet the standard of GDPR consent, then Operators must assess whether the processing may be based on a different legal basis, taking into account the conditions laid down in the GDPR. If an Operator is unable to renew consent in a compliant way, and is also unable to make the transition to GDPR compliance by basing data processing on different legal basis while ensuring that continued processing is fair and accounted for, the processing activities must be interrupted. In any event the controller needs to observe the principles of lawful, fair and transparent processing. However, in the event that the previously-obtained consent meets the standards of GDPR consent, and the purposes of the data processing will be unchanged with regard to the consent which has already been obtained, it is not necessary for a B2C licensee to obtain a new consent. Having said this, the controller is still required to inform the data

[2] WP 29 Guidelines on Consent, page 12.
[3] Recital 42 GDPR.

subjects about the new privacy terms, including the applicable rights, in line with the transparency requirements set out under Article 13 of the GDPR.

As a general rule, if consent is withdrawn, all data processing operations that were based on consent and took place before the withdrawal of consent - and in accordance with the GDPR - remain lawful, however, the controller must stop the processing actions concerned. If there is no other lawful basis justifying the processing (e.g. further storage) of the data, they should be deleted or anonymised by the data controller[4].

4.4 Legitimate Interest

A data controller may rely upon legitimate interest as legal basis for the processing of personal data, subject to identifying a legitimate interest, establishing that the processing is 'necessary' and conducting a balancing test. Legitimate interests can be those of the controller or a third party to whom the personal data may be disclosed.

Operators should consider whether that processing is necessary for the pursuit of their commercial or business objectives (i.e. there does not appear to be another way of achieving the identified interest), and then confirm, by means of a balancing test, that the rights and freedoms of the player whose personal data will be processed have been evaluated, and that these interests do not override the Operator's legitimate interests, taking into account, for example, the scale of data collection, the nature of the interests, the impact of the processing and any safeguards which are or could be put in place such as data minimisation, de-identification and data retention limits. If a player could not reasonably expect the processing, or if the processing causes unjustified harm, the player's interests will override the Operator's 'legitimate' interests.

Practical scenarios: this is a broad, non-exhaustive list of examples, intended to give an illustration of scenarios in which Operators may consider the use of legitimate interests as the basis for the processing of personal data. All of these examples would be subject to the Operator conducting its own balancing test in accordance with Article 6(1)(f) of the GDPR.

a) **Fraud** - An Operator wants to process a player's personal data as part of its business critical anti-fraud measures. Although this is undoubtedly in the interests of the Operator, it could also be seen as benefitting other players, since the cost of fraud results in the restrictive offer of bonuses and promotions generally.
b) **Risk Assessment** - Operators need to "risk assess" all their players for a number of scenarios envisaged by separate legal obligations, including but not limited to anti-money laundering (AML) and player protection obligations. However, risk-assessment are also carried out in order for Operators to determine the nature of the products and services they are offering, and the terms of those services. Although details of such processing should be included within the privacy policy, it is not required that an Operator seeks consent for such risk-assessment-related processing.

[4] WP 29 Guidelines on Consent, page 22.

c) **Players who have opted-out of receiving marketing communications** - In order to ensure that a player who has opted-out of receiving marketing communications, but has not self-excluded, receives no marketing communications, that player's data must be held on a suppression file. The legitimate interest ground may be satisfied here, as long as the Operator holds the minimised amount of personal data possible in order to uphold this request.
d) **Network security** – Any network security activity undergone by an Operator and which is considered to be an essential processing activity by the Operator, which activity is intended to ensure that its customers are continually protected.
e) **Personalisation and web-analytics** – An Operator may rely on legitimate interests to justify non-personalised analytics to inform its marketing strategy and to enable it to enhance and personalise the "gaming experience" it offers to its players (in line with the relevant Commercial Communications legislation).
f) **Non-invasive profiling for direct marketing** – While an Operator should generally rely on consent for marketing communications, it may rely on legitimate interest for clustering customers based on age group, location and game history for direct marketing purposes, provided that the level of intrusiveness of the profiling is low and the appropriate measures (including security measures and easy to use opt-out tools) are adopted to strengthen the legitimacy of the processing and to genuinely balance the interests of the Operator with the reasonable expectations of the players. However, when in doubt as to whether to rely on consent or legitimate interest, it is advised that you seek guidance from your Lead Supervisory Authority (LSA).
g) **Customer Support logs** – Even when the storage of such logs are not mandated by law, the information within the logs may be used to manage disputes with players, to direct players to responsible gaming support staff, and to improve the players' experience. Such logs could also be used to identify recurring software issues, and to analyse the patterns of behaviour of customers and staff provided that an adequate balancing test has been carried out and such analysis does not comprehend invasive profiling.
h) **Artificial intelligence and machine learning** - An Operator can put in place a system which uses artificial intelligence and neural network to route customer communications to the most appropriate part of the organisation. These routes could link individuals to specific agents who can handle specific requests, but in addition the algorithm might ask a series of questions and provide appropriate answers without the need for human intervention. The system by processing personal data of the individual would learn to optimize its suggestions and answers.

Operators relying on legitimate interests as the basis for fair processing must maintain a record of the assessment they have made, so that they can demonstrate that they have given proper consideration to the rights and freedoms of data subjects in their determinations.

Additionally, it should be noted that the presumption of legitimacy may be challenged by an individual (or group of individuals), in which case the processing must stop unless the controller can show compelling grounds to continue with the processing which override the individual's rights, or alternatively if the processing is needed to establish, exercise or defend legal claims.

5 Data Subjects' Rights

The GDPR enshrines the various rights of data subjects to be observed and respected by controllers and processors of personal data. The manner in which some of these rights are applicable to the industry is outlined below:

5.1 Right to be Informed

The GDPR imposes a general obligation of transparency. Operators must be transparent on the data they are processing by providing clear, concise, intelligible and easily accessible information notices to all their players. These information notices, also known as privacy policies, are to be brought to the attention of the data subject whose data is being processed by an Operator.

5.2 What should a privacy policy include?

Privacy policies should include the following minimum information:

a) Identity and contact details of the data controller, i.e. the Operator, who determines the purpose of the processing and, where applicable, of the controller's representative, as well as the contact details of the Operator's Data Protection Officer (DPO).
b) Purposes of processing and legal basis for processing – including the "legitimate interest" pursued by the controller (or third party) if this is the legal basis chosen, i.e. the specific interest in question must be identified. Furthermore operators should make clear to players that they can obtain information on the balancing test, at the basis of the legitimate interest, upon request[5].
c) An Operator's privacy policy should also inform players or potential players that when an account is opened, the player(s) personal data may be processed for anti-money laundering (AML) purposes, particularly in light of the exception detailed below.
d) Recipients, or categories of recipients. This includes other data controllers, joint controllers and data processors to whom data is transferred or disclosed. The default position is that a data controller should provide information on the actual (named) recipients of the personal data. This means that the data processors should be listed in the privacy policy. Where a data controller opts to only provide the categories of recipients, the data controller must be able to demonstrate why it is fair for it to take this approach. In such circumstances, the information on the categories of recipients should be as specific as possible by indicating the type of recipient, for instance, by reference to the activities it carries out.
e) Details of data transfers outside the EU and the reference to the appropriate or suitable safeguards. The data subject shall be provided also with the means to obtain a copy of them or details as to where they have been made available (e.g. link to the website page of the Standard Contractual Clauses).
f) The retention period for the data, or, if no period can be possibly set, the criteria used to set this. It is not sufficient for the Operator to state that the personal data will be kept for as long as necessary for the legitimate purposes of the processing.

[5] WP 29 Guidelines on Transparency, page 36.

g) That the player has a right to access his/her data, as well as rectify, erase and restrict it, as well as to 'port' it (see right to data portability below).
h) That the player has a right to object to the processing or his/her data, and to withdraw consent, if the processing is based on consent.
i) The possibility of a player to lodge a complaint to a supervisory authority. This information should explain that, in accordance with Article 77 of the GDPR, the player has the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of an alleged infringement.
j) Whether there is a statutory or contractual requirement to provide the data and the consequences of not providing that data (only applicable in relation to data collected directly from the data subject). For example, upon registration, online forms should clearly identify which fields are "required", which are not, and what will be the consequences of not filling in the required fields.
k) Whether or not there will be any automated decision taking, and if so, information about the logic involved and the significance and consequences of the processing for the player. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling together with meaningful information about the logic involved and the significant and envisaged consequences of the processing for the data subject.

5.3 When is the privacy policy to be notified, and/or brought to the attention of the player?

As a general rule, a privacy policy is to be brought to a data subject's attention when his/her data is collected and also during the course of the Operator-player relationship.

Changes to a privacy policy should always be communicated if they include substantive modifications (i.e a change to the identity of the controller or a change as to how data subjects can exercise their rights in relation to the processing.) The GDPR provides further guidance as to when such information must be provided. Specifically, this depends on the time as to when this data is collected: if this data is collected directly from the player, then all the information must be provided at the time that the data is obtained. If the Operator does not obtain this data directly from the player, then the Operator, in addition to informing the subject of the source(s) of the information, even if it came from publicly accessible sources, must provide such information:

i. within a reasonable period of having obtained the data, but not later than one month from having received it;
ii. if the said data is used to communicate with the individual, not later than when the first communication takes place; or
iii. if the data is to be disclosed to another recipient, before such data is disclosed.

Given the long list of contents which are to be included within a privacy policy, it is understandably challenging to provide the information efficiently and succinctly, however the below points are intended to provide further guidance to assist Operators to fulfil their GDPR obligations in this regard:

a) The information should be clearly differentiated from other non-privacy related information, for example contractual provisions or general terms and conditions of use.
b) Intelligibility is closely linked to the requirement to use clear and plain language. To this extent, an accountable data controller will have knowledge about the people they collect information about and it can use this knowledge to determine what that audience would likely understand[6].
c) Online Operators should 'layer' the information. This will enable a player to easily navigate through headings of information within the privacy policy, and access any particular point which he/she would like more detail on.
d) Within the registration-page, prior to registering as a player, the privacy policy should be brought to the attention of the player.
e) Once the player has registered, and throughout the player's use of the website, online Operators should provide a link to the privacy policy on every page of the website. In the case of applications, the information should be made available on the online store prior to purchasing the product. Once the app is installed, the information still needs to be easily accessible from within the app. Additionally, the privacy information in question should be specific to the particular app and should not merely be the generic privacy policy of the company that owns the app or makes it available to the public. Generally speaking, the entire privacy policy should not be more than two clicks/ two taps away.
f) Land-based Operators should attach a printed copy of the privacy policy to the registration form, where this is provided in hard-copy. If the form is filled on a computer device, a tablet or similar tool, the registration form should include a link to the privacy policy.
g) When data is being collected from a data subject, the link to the policy should be immediately accessible[7].
h) The language must be as clear, and simplistic as possible, devoid of abstract or ambivalent terms.
i) The purposes of, and legal basis for, processing the personal data should be clear. Words such as "may", "might", "some", "often" and "possible" should be avoided. Where data controllers use indefinite language, they should be able to demonstrate why the use of such language could not be avoided and how it does not undermine the fairness of processing.
j) The privacy policy should be in the English or Maltese language, and in all the languages of the countries in which the Operator is providing the service.

5.4 When can an Operator process a player's data without informing the player that such processing is taking place?

Articles 13 and 14 of the GDPR also provide a short list of exceptions to this obligation to provide information. With regard to data which has been collected from the individual, the only exception occurs when and insofar as, the data subject already has the information[8]. Given that, within the gaming

[6] WP29 Guidelines on Transparency provide an example: "a controller collecting the personal data of working professionals can assume its audience has a higher level of understanding than a controller that obtains the personal data of children".
[7] WP 29 Guidelines on Transparency, page 8.
[8] Article 13(4) of GDPR.

industry, most of the time data will be collected from the player at registration stage, it is unlikely that the player would already have the privacy policy. Any time the player provides additional data to the Operator after registration stage, although not necessarily required by law, it would be considered best practice if the privacy policy is brought to the player's attention once more.

Where personal data has not been collected from the data subject, an Operator may be exempt from providing information regarding the processing of the data if:

a) The provision of such information would make the achievement of the objectives of the processing impossible, or seriously impair them. To rely on this exception, Operators must demonstrate that the provision of the information alone would nullify the objectives of the processing. Of course there would need to be legal basis for the processing of the data, and it must be done in a fair manner. To this end, such instances will be laid down within further legal instruments issued under the Data Protection Act.

For example, Operators are subjected to a mandatory requirement under Anti-Money Laundering (AML) legislation to report suspicious activity relating to accounts held with it to the relevant gaming and/or financial authority. The AML legislation in question makes it a criminal offence for a reporting Operator to "tip-off" the account-holder that may be subject to regulatory investigations. Such a scenario qualifies as an exception, however upon registering an account, all account-holders should have been provided with general information informing them that the players' personal data may be processed for AML purposes.

b) Obtaining or disclosing the data is expressly laid down in the law. To qualify for this exception, data Operators must be able to demonstrate how the law in question applies to them, and requires them to either obtain or disclose the personal data in question. However, the Operator should make it clear, within the privacy policy, that it obtains or discloses personal data in accordance with the applicable law, unless there is a legal prohibition preventing the data controller from doing so.

5.5 Right of access

This right is intended to empower data subjects to be aware of the personal data being processed and to be able to verify the lawfulness of that processing.

Under the GDPR, data subjects will have the right to obtain:

a) Confirmation that data about them is being processed;
b) A copy of their personal data undergoing processing; and
c) Other supplementary information, including information on appropriate safeguards in place when transferring data.

Players have a right to request access to their personal data in the gaming industry, when taking into account that Operators process large quantity of information concerning their clients. Upon receiving a Subject Access Request (SAR), a B2C licensee should be able to ask the data subject to specify the information or processing activities to which the request relates. However, if such a subject access request is not limited, then a B2C licensee must provide such information as required by the GDPR.

For the purposes of facilitating subject access requests, Operators may consider providing data subjects with remote access to a secure system which would provide the data subjects with direct access to his or her personal data.

The data subject must be given a reason when the Operator does not intend to comply with the request and also provided with the necessary information on the possibility to lodge a complaint with the supervisory authority and seeking a judicial remedy.

The GDPR makes it clear that the right to obtain a copy shall not adversely affect the rights and freedom of others. Furthermore, Operators can refuse to provide that information which reveals trade secrets, intellectual property and, in particular, copyright protecting software.

5.6 Right to rectification

The data subject has the right to have inaccurate personal data about him corrected. The data controller must take every reasonable step to ensure that inaccurate personal data is rectified or deleted.

Operators must respond to a request for rectification within one month. The data subject must be given a reason when the Operator does not intend to comply with the request and also provided with the necessary information on the possibility to lodge a complaint with the supervisory authority and seeking a judicial remedy.

5.7 Right to Data Portability

The newly introduced right to data portability imposes two new obligations on the controller. Upon data subjects' request, the controller shall:

a) forward to the data subjects the personal data which they have received from the same data subject, in a structured, commonly used and machine-readable format; and
b) transmit those data to another data controller, where it is technically feasible to do so.

Controllers should consider having download tools or API setups – data must be transmitted in a structured, commonly used and machine-readable format. The GDPR encourages controllers to have interoperable formats, however this is not an obligation to adopt or maintain processing systems which are technically compatible. In the absence of any format common to the industry, controllers are to provide the data using commonly-used open formats (e.g. XML, JSON, CSV, etc). Upon selecting a format, the Operator should consider how this format would impact or hinder the individual's right to re-use the data. Controllers should keep in mind, however, that they are prohibited from establishing barriers to the transmission, even if the request relates to sending over a player's data to a competitor. Any potential business risk cannot serve as the basis for a refusal to answer the portability request, and

controllers must seek to transmit the personal data in question in a format which does not release information covered by trade secrets or intellectual property rights[9].

If the data is handled by another party on the data subject's behalf, the other party is to be considered a controller, even for the sole purpose of data storage.

This right of the players complements the right of access to their data. If Operators ensure that such data is stored in an easily accessible manner, then it would be significantly easier, and much less burdensome, for them to comply with both rights. However, it should be noted that portability is a narrower right than subject access. It only applies to:

a) personal data which is processed by automated means, and therefore excludes any paper records;
b) personal data which the data subject, i.e. the player, has provided to the controller; and
c) only to cases where the basis for processing is consent, or that the data is being processed to fulfil a contract or steps preparatory to a contract.

In industry terms, data which falls under this rights includes all player data submitted by the player upon registration, and any data which the player would have passed on to the Operator in the course of any dealings between the two, or even personal data which has been generated by the Operator from observation of the player's activity, such as activity logs and history of website usage. Any history of self-exclusion or wager, loss or deposit limits should also be considered personal data which can be transferred by virtue of this right. However, the right does not extend to personal data inferred or derived by the Operator, for example the results of an algorithmic analysis of the individual's gaming behaviour, or a player's profile kept by the Operator in the context of risk-management and financial regulations. Neither are Operators obliged to answer a data portability request concerning personal data processed as part of their obligations to prevent and detect money laundering and financial crimes, and manipulation of sports competitions, where law dictates such obligations[10].

It must also be noted that data portability must not prejudice any other right held by the player (this rule applies to all rights in the GDPR). It means that if the data is requested by the player, or a player requests the Operator to transfer his/her data to another controller, the Operator should not erase that data from its systems, and the original retention period applying to the data which has just been transmitted, remains applicable. It therefore follows that the same player may exercise any other applicable right under the GDPR in relation to that data. Furthermore, data portability right shall not prejudice the right of the data subject to obtain the erasure of personal data and the exercise of this right shall not be used to delay or refuse any request to erase such data under the GDPR's right to erasure.

For example, if a player is undergoing a self-exclusion period, but he/she submits a request to have his/her data sent over to another operator, in addition to including the self-exclusion data within the set of data, the operator must remain compliant with its responsible gaming obligations. To this end,

[9] WP29 Guidelines on right to data portability, page 12.
[10] Recital 68 of GDPR.

an operator who receives such a request from a player undergoing self-exclusion should ensure that responsible-gaming professionals within its operation make contact with the player, and refer such player to responsible-gaming bodies, or problem-gambling treatment facilities, in accordance with the respective gaming laws.

The right to data portability shall not adversely affect any rights and freedoms of other individuals. Therefore, if a set of personal data concerns data pertaining to more than one data subject, his/her right to receive that data should not prejudice the rights enjoyed by the other data subject under the GDPR. If an Operator were to receive a player's personal data from another controller, and this includes data relating to a third person which the player would have provided to the latter, the receiving Operator may not use such information to enrich the profile of such a third party data subject without his knowledge and consent[11].

Upon delivery the personal data, the Operator sending the data is responsible for taking all the security measures needed to ensure not only that personal data is securely transmitted (end-to-end encryption) to the right destination (by the use of strong authentication measures), but also continuing to protect the data that remains in their systems. The Operators should assess the risks linked with data portability and take appropriate risk-mitigation measures, such as authentication mandate in cases of direct transmission to another data controller[12].

It is recommended that all controllers implement tools which enable the respective data subjects exercising this right to exclude, where relevant, the data of other individuals.

Operators must inform all players of the existence of this new right to portability (i.e. it shall be made explicit within the privacy policy). It is recommended that this is done at registration stage, when the player is entering into a contractual relationship with the Operator, and thereby providing personal data. If the player provides additional data at a later stage, or if the data has been forwarded by another individual, the Operator must communicate the said right to the player as soon as possible. Operators should distinguish the precise nature of the data which is subject to this right. It is also recommended that Operators notify the players of this right upon receiving a request to close the player account.

Upon receiving a request, Operators are obliged to reply "without undue delay" and in any event "within one month of receipt of the request."[13]. This also includes instances wherein the Operator denies such a request. In such a case, the Operator is to inform the player with regard to the "reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.[14]"

It is not permissible to charge a fee for compliance with such a request, although if an Operator can demonstrate that the requests are manifestly unfounded or excessive, then a fee can be considered.

[11] WP 29 Guidelines on Data Portability, page 12.
[12] WP 29 Guidelines Data Portability, page 19.
[13] Article 12(3) of GDPR.
[14] Article 12(4) of GDPR.

However, it should be kept in mind that the group of European data protection authorities, the Working Party ex. Article 29 (in the following "WP29") recognised in its Guidelines that the setting up of an API facilitates these exchanges, and it is unlikely that any requests would be considered “excessive”. As a general rule, therefore, Operators should steer clear of seeking to charge any fees in this regard.

Interestingly, this right is also applicable to players who share gameplay footage. Having said that, it does not appear this right results in a requirement to retain personal data beyond the usual retention period, therefore if a platform’s approach is to only stream live play-through footage, and to delete such footage from the servers once the play-through is complete, then there is no obligation on the platform to retain the data.

Data processors are contractually obliged to assist controllers “by appropriate technical and organisational measures” with regard to responding to data portability requests. It is advisable that processors and controllers consider the setting up of specific procedures in relation to such requests.

It should be noted that WP29 Guidelines stress that if a player makes it clear that he/she is making a request not under the GDPR, but rather under any other sectorial legislation, such as the Payment Services Directive 2, then the access should be granted according to such sectorial legislation, and not the GDPR’s data portability provisions[15]. It is evident that any interplay between rights would need to be assessed on a case-by-case basis, however, it is recommended that guidance is sought from the Operator’s Lead Supervisory Authority in any instances wherein the GDPR’s data portability requirements conflict with other access and portability requirements or member state legislation. Operators should not automatically assume that sector-specific legislation automatically displaces any GDPR right.

5.8 Right to Object

Data subjects have the right to object to:

a) Processing based on legitimate interests or the performance of a task in the public interest or in the exercise of official authority;
b) Direct marketing, including profiling to the extent that it is related to such marketing activities; and
c) Processing for scientific or historical research purposes or for the purpose of statistics.

Following an objection, the controller may no longer process the personal data unless the Operator demonstrates compelling legitimate grounds which override the interests, rights and freedoms of the data subject or in order to establish, exercise or defend legal claims. However, it is the controller who bears the burden of proof for demonstrating such compelling interests that override the rights of the data subject and the data subject is therefore not precluded from objecting.

If a player objects to processing for direct marketing purposes, B2C licensees must stop processing the personal data for such purposes as soon as the objection is received; there are no exemptions or

[15] WP29 Guidelines on Data Portability, pages 7-8.

grounds to refuse. In the case of the use of information society services, the data subject may exercise his right to object by automated means using technical specifications.

A B2C licensee always has the right to terminate a player's account (in accordance with the regulations and procedures mandated by respective gaming laws to which the licensee is subject) in the event that it would not like to proceed with offering the gaming service once it has received such objections, particularly in relation to processing based on legitimate interests, if this were to significantly affect the service it would provide to the particular player in question, or to its customers in general.

The right to object must be clearly brought to the players' attention. The player is to be informed of this right at the time of the first communication, and within the B2C licensee's privacy policy, and this is to be presented to him/her clearly and separately from any other information.

If any of the processing activities are carried out online, the data subjects must be offered a way in which to object online.

6 Automated Decision-Making and Profiling

Profiling is a procedure that includes any form of automated processing of personal data which may involve a series of statistical deductions. It means gathering information about an individual (or group of individuals) from different sources and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group to analyse and/or make predictions about, for example, their ability to perform a task, preferences, interests or likely behaviour.

Automated decision-making has a different scope, and may partially overlap with profiling, but such decisions can be made with or without profiling, and profiling can take place without making automated decisions. However, something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used.

As a rule, in order to prevent individuals from being subject to decisions taken by machines that could influence their lives, article 22 of the GDPR prohibits fully automated individual decision-making, including profiling, that has a legal or similarly significant effect.

Within the gaming 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. An automated-decision is said to similarly significantly affect a data subject if the decision has the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned.

However, there are exceptions to the rule and notably, Recital 71 of the GDPR specifies that automated decision making and profiling are allowed where expressly authorized by Union or Member State law to which the Operator is subject, and this would include fraud, tax evasion and suspicious betting pattern reporting. However, even though such processing may be mandated by law, it is highly recommended that Operators dedicate an element of human intervention in making decisions about players which have a legal or similarly significant effect on the player, such as refusing him as a player, or reporting him to the Authorities and there should be measures in place to safeguard the data subject's rights,

freedoms, and legitimate interests, for example by informing them within the privacy policy (as explained in Section 5 above).

If an Operator would still like to proceed with such automated decision making, it could seek a player's specific and explicit consent, and this would also serve as an exception from the prohibition.

If an automated process produces what is in effect a recommendation concerning a player, but a human being within the Operator's organisation reviews, and takes account of other factors in making the final decision, then that decision is not 'based solely' on automated processing, and is not captured by the prohibition under Article 22[16]. It should be noted that if no human has any decision-making power, irrespective of whether said human is otherwise involved in the decision making process, such as by scanning decision-relevant documents, the prohibition still applies.

7 The Controller-Processor Relationship

The GDPR imposes a high duty of care upon controllers in selecting their personal data processors.

The controller should only contract with processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources to implement technical and organisational measures that will meet GDPR requirements, including for the security of processing. In other words, Operators shall only choose processors that comply with the GDPR, or they could risk penalties themselves. The controller-processor relationship should be governed by a contract or other legal act, binding the processor to the controller, which, *inter alia*, sets out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, the manner in which the processor will report any data breaches to the controller, the steps which will be taken by the processor to secure the data, the specific tasks and responsibilities of the processor and the risk to the rights and freedoms of the data subject. Both controllers and processors must ensure that the contract laying down the terms for their service is in line with the GDPR.

Gaming Operators, as controllers, must therefore ensure that cloud services providers only process personal data for the purposes as initially agreed in their controller-processor agreement and as identified with the data subject.

If the processor wishes to engage another processor, which may be referred to as a "sub-processor", the processor must obtain the prior approval of the controller. This applies even if you have a general consent to sub-contract, so as to give the data controller the opportunity to object. In this case, the same data protection obligations set out between the controller and the processor must apply to the relationship between the processor and sub-processor. If the sub-processor fails to fulfil its data protection obligations, the initial processor remains fully liable to the controller for the performance of the sub-processor's obligations[17]. In respect to the relationship between Operator and affiliate, the latter should be instructed not to engage another processor (i.e.: another sub-affiliate) without prior specific

[16] WP 29 Guidelines on Profiling, page 9.
[17] Article 28(4) GDPR.

or general written authorization of the controller – i.e. the Operator. The GDPR allows more flexibility in appointing sub-affiliates, but such flexibility still requires that Operators must be able to have at any time a full picture of the data processing activities performed on their behalf.

Where two or more controllers jointly determine the purposes and means of processing, they are considered to be joint controllers. Together, in a transparent manner, they determine their respective responsibilities for compliance with the GDPR. As detailed below, this could be the case with affiliates, for example.

Controllers of personal data, and where applicable, the controller's representative, must also maintain a record of processing activities under their responsibility[18]. On the other hand, processors of personal data, and where applicable, the processor's representative, must maintain a record of all categories of processing activities carried out on behalf of a controller. Each controller and processor should be obliged to cooperate with the Information and Data Protection Commissioner (in the following "IDPC") and make those records available to it on request.

7.1 Affiliates

Affiliates may be both processors and controllers. Their classification depends on the nature of the processing which they carry out. It could be said that an affiliate who reaches out to prospective players and proceeds to provide those customers to an Operator, has complete autonomy over the processing of the customers' data, and is hence a controller. When an affiliate solely acts on behalf of the Operator, by driving traffic towards that Operator, and when such an affiliate would not have otherwise been processing that data had it not been for his relationship with the Operator, then that affiliate is acting as a processor. There are situations where affiliates are acting as both controllers and processors in the course of conducting marketing activities. This may be the case when affiliates compile their own mailing list and then use it to send promotional material on behalf of operators. There is also the possibility that the Operator and its affiliate are considered to be joint controllers, if they are deemed to be jointly determining the purposes and means of processing.

Therefore, in the case of a breach, one would need to determine the precise nature of the processing being carried out by the affiliate when the breach was made, however, the GDPR introduces liability for both processors and controllers, thus lessening the impact of determining whether an affiliate is a controller or a processor. However, the LSA is the body which will ultimately determine the precise role of an affiliate in coming to a conclusion. It must be reminded that under Malta's gaming laws and regulations, both a licensee and a third party carrying out marketing can be found responsible for any breach, and a breach by a third party carrying out a function on behalf of a licensee may nevertheless affect the standing of a licensee with the Authority.

To this end, it is being reminded that licensees are to ensure that the contents of their agreements with affiliates and third parties alike, reflect the responsibilities required by both entities, and demand compliance with gaming and data protection legislation. Together and in a transparent manner,

[18] Article 30 GDPR.

Operators and affiliates should determine their respective responsibilities for compliance with gaming laws and with the GDPR.

The main principles of the matter just examined above, can be summarized as follows:

1. Players can file direct claims for breach of their privacy rights against both Operators and their gaming affiliates if the breach is the result of the conduct of affiliates.
2. Gaming affiliates' liability arises if they did not comply with the obligations imposed specifically on them directly by the GDPR, or by the lawful instructions of the Operator, when acting as processors.
3. Depending on the affiliate model, the operator, the affiliate or both will have the burden of proof to demonstrate compliance with the data protection law.
4. In case of more than one Operator or affiliate, each of them may be found liable for damages.
5. Gaming affiliates are responsible for the conduct of the sub-affiliates appointed by them (i.e. of the network of affiliates reporting to a "master" affiliate).

7.2 Security measures

When acting as processors, affiliates are obliged to notify any data breach to the Operator without undue delay after becoming aware of a personal data breach. However, since Operators are obliged to notify data breaches to the LSA not later than 72 hours after having become aware of it, if an affiliate is not able to identify and does not notify a data breach to the Operator within less than 72 hours from its occurrence, it might be considered to be evidence of a lack of compliance with GDPR.

In those cases where an affiliate suffers a data breach in relation to its own records (e.g. marketing database), for which it is responsible as a data controller, such affiliate shall notify the breach to the supervisory authority within 72-hours from becoming aware of the breach.

8 Marketing

8.1 Unsolicited marketing

Maltese gaming laws prohibit any Operator from engaging in any activity that involves the sending of unsolicited commercial communications, whether it is through its own operation or by the intervention of third parties.

8.2 Solicited Direct Marketing

Operators, and any third party engaged by the operator, are responsible for ensuring that the processing of data for the purpose of direct marketing is based upon an appropriate legal basis as required within the GDPR. In the case of marketing communication sent by electronic means, the processing must comply with the rules of Directive 2002/58/EC (transposed in national law by virtue of S.L 440.01) which

will eventually be superseded by the ePrivacy Regulation. These guidelines suggest the following set-up[19]:

The registration screen of every operator, besides requiring registering players to agree to terms and conditions, should also include a tick-box which enables the said individuals to opt-out of receiving marketing communications from the same operator, or from any processor processing player data on the Operator's behalf for the purposes of sending out any marketing communications. This approach is commonly referred to as opt-out or soft opt-in. Where the opt-out approach is adopted, the operator or a processor engaged for such purposes shall only send marketing communication in relation to similar products or services for which the individual made initial contact.

A separate tick-box seeking the registering player's opt-in consent is required if the Operator will be transferring to or sharing that data with any third parties, including to any other data controllers within the same group of companies, as well as to receive marketing communications from the said third parties.

8.3 Marketing carried out by third parties, including by affiliates

When engaging affiliates to conduct marketing activities on their behalf, Operators should have in place a due diligence process, which includes the assessment of their data protection practices, the consent mechanisms for direct marketing, including documented evidence to prove consents, the privacy policy and the provision of unsubscribe options. Such procedures shall also be monitored on an ongoing basis in order to ascertain that the entrusted affiliates are complying with the applicable data protection laws.

Furthermore, when a communication is sent by an affiliate on behalf of an operator, this should be made clear to the data subject, and such communication shall facilitate an easy opt-out method.

9 Data Retention

The period for which the personal data is stored should be "limited to a strict minimum.[20]". The impact of the GDPR on the retention of personal data is particularly problematic in the gaming industry in light of legal obligations imposed on gaming Operators by various legal instruments, and separate rules and obligations. Operators are required to specify "the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period[21]" within their privacy policy. In compliance with the so called "risk based approach" Operators shall be able to justify the data retention periods that have been determined on the basis of the criteria.

Operators therefore have the obligation to determine the relevant data retention period. There is no one period which is suitable for all Operators, nor for all players registered with the different Operators, and

[19] Kindly be reminded that the below should not be interpreted to mean that this is the only correct manner in which this processing can be carried out. Neither is it guaranteed that every supervisory authority will adopt the same interpretation.
[20] Recital 39 GDPR.
[21] Article 13(2)(a) GDPR.

the applicable period depends on the type of data which is being processed, and the purposes for that processing. As general guidance, however, data pertaining to a player who closes his/her account with a gaming company, and who is not undergoing an indefinite self-exclusion period, should not be retained beyond the years mandated by applicable AML/CFT legislation, unless there is justification for doing so. An example of such justification includes the suspicion that such a player has been involved in organised crime by virtue of his/her gaming activities, while the fact that such a player has abused of bonus schemes, or was otherwise fraudulent, is not considered as justification for retaining the data beyond AML/CFT requirements. In order to determine the correct data retention period only the purposes, not instruments, of the processing must be taken into consideration.

For example, in order to determine the correct data retention period in the case of processing personal data by e-mail, the Operator shall take into consideration only (i) the categories of personal data; (ii) the purposes of the processing; (iii) the type of business in which the company operates. The functionality of the email software (which is precisely a tool and not a purpose) has no legal significance.

A policy on the retention applicable to different categories of personal data shall be adopted in line with the principles of the GDPR. The policy shall outline: (i) mandatory retention requirements; (ii) how and when data should be deleted or anonymised; (iii) the security measures which should be adopted as part of such activity.

Once the periods are determined, Operators must set up a data management system, made up of technical and organisational measures which enable the company to comply with other GDPR obligations in relation to that data, including data minimization, data portability requests, the management of data breaches, and the right of erasure.

The current EU Data Protection Directive 95/EC/46[22] already requires Operators to minimize the retention of personal data in identifiable form when this is no longer necessary for the purposes for which the data are collected or processed. The GDPR reiterates this principle[23] while also requiring that personal data may be stored for longer periods insofar as it is processed for archiving purposes in the public interest[24], subject to implementation of the appropriate technical and organisational measures required by the same Regulation.

What this means for B2C Operators in the gaming industry essentially depends on the categories of personal data which they are processing. Additionally, Operators must ensure that they are only holding

[22] Article 6(1)(e) Directive 95/EC/46.
[23] Article 5(1)(d) GDPR.
[24] As well as for scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

data which is relevant and limited to what is necessary. The data should also be subject to periodic review in order to evaluate whether or not it is still justified to keep that data.

Personal data of players who have had their accounts closed, or who have voluntarily closed their accounts, and who would be accepted as players by an Operator should they choose to re-register as players, should be erased or completely anonymised upon the lapse of any retention period mandated by law, such as anti-money laundering legislation.

For example, a gaming operator holds personal data about its players. This includes details of each player's name, surname, date of birth, bank account number. The gaming website uses this information as part of its security procedures. It is appropriate for the gaming website to retain this data for as long as the player has an account with the website. After the account has been closed, the operator may need to continue holding some of this information only for legal or operational reasons, with the periods and the said reasons included within the privacy policy.

9.1 Right of Erasure

The Right of Erasure, commonly known as the right to be forgotten, is granted to individuals who make a request to have personal data pertaining to them erased and free from further processing, only in the following circumstances:

a) the personal data is no longer necessary for the purpose for which it was collected or processed;
b) the data subject withdraws consent, and there is no other legal ground for the processing;
c) the data subject objects to the processing and there are no overriding legitimate grounds;
d) the personal data was unlawfully processed;
e) the personal data has to be erased to comply with a legal obligation of the controller; and, or
f) the personal data was collected in relation to the offer of information society services to a child.

The controller, however, is not bound to comply with a request for erasure if the processing is necessary:

a) to exercise the right of freedom of expression and information;
b) to comply with a legal obligation or to perform a task carried out in the public interest or in the exercise of official authority; and, or
c) to establish, exercise or defend legal claims.

Therefore, in line with the above requirements, such requests in relation to, inter alia, data pertaining to self-excluded players, data retained in order to prevent fraudulent players from re-registering with a gaming website, or from re-entering a gaming premises, data maintained in relation to sports-betting integrity cases, or data maintained in order to fulfil an obligation maintained by any other law, such as money-laundering legislation, should generally not be entertained This is without prejudice to the data retention period determined on the basis of the criteria as explained above.

However, it is the Operator's duty to erase that data whenever none of the above circumstances remain applicable. Furthermore, a request for erasure which cannot be upheld, should lead to a re-examination

of the relevant player's profile, and any data which is unnecessary should be anonymised, pseudonymised or de-identified.

For example, in case of impracticable deletion, alternative interventions could be envisaged, such as: (i) access to copies only in cases of emergency and restoration; (ii) preservation of supports, appropriately encrypted.

10 The Cross-Border Processing of Personal Data, within, and outside, the EU/EEA

10.1 Intra-Group Transfers of Personal Data within the EEA

The free exchange of personal data between Member States is a fundamental aspect of the EU's basic principles. This principle is also reflected in the GDPR, which excludes the restriction or prohibition of the free movement of personal data within the EU or EEA. In the case of intra-group data transfers, therefore, no other particular restrictions apply. That said, data transfers between different group members require a legal basis and thus are regarded as any other transmission or disclosure under this point of view.

The GDPR also recognises that controllers forming part of a group of companies can have a justified interest in transferring personal data within their group for internal administration purposes, including the processing of personal data of players and employees. So, even though there is no kind of "intra-group privilege" under the GDPR, intra-group data processing is in any case facilitated to a certain extent. Some of the organisational and material requirements can be implemented in a simplified manner by the group entities. On the other hand, group entities face enforced data protection obligations if the processing activities of different controllers are linked, as this will require a careful allocation of responsibilities.

10.2 Transfer of Personal Data outside the EEA

The GDPR imposes restrictions on cross-border processing of personal data to non-EU countries or international organisations to guarantee the data subject's adequate protection over his/her personal data.

As a general rule, transfers of player data to a country outside the EU may take place where such a country has been designated as one which ensures an adequate level of protection, i.e. Adequate Jurisdictions[25]. In summary, entities must verify in a two-step approach that this processing activity is covered by a legal basis and that appropriate safeguards will be applied to such transfer. These

[25] At the time of publication, The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework) as providing adequate protection.

safeguards, under the GDPR, shall provide for conditions for onward transfers that shall help to keep up an appropriate level of data protection similar to the one under the GDPR in case of such transfers.

There are a number of instances, however, where data is to be processed outside the EU/EEA and where no 'adequacy decision' has been reached. This is equally applicable for the processing of data by cloud service providers, among others. In such cases, licensees transferring personal data to such countries must have the appropriate safeguards in place.

a) Model data protection clauses: At the time of publication of these Guidelines, the Commission has issued two sets of contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU/EEA, and for data transfers from controllers in the EU to processors established outside the EU.EEA. These clauses are available for download from the EU Commission's website[26]. The use of the model clauses does not prevent Operators or processors from adding to these clauses, provided that there is no contradiction between the clauses. Therefore, the GDPR does not tolerate any standard format data processing agreements. Operators are obliged to renegotiate the data processing agreements. Indeed, GDPR provides for a detailed list of instructions that have to be contained in the relevant agreement.
b) Binding Corporate Rules ("BCRs"): where a member of the corporate group of a licensee is itself established outside the EU/EEA, and outside a country subject to an Adequacy Decision, the BCRs allow the transfer of personal data internationally within the same corporate group while ensuring that all data transfers are safe. The BCRs must contain: (i)privacy principles, such as transparency, data quality, security; (ii) tools of effectiveness (such as audit, training, or complaint handling systems); and (iii) an element proving that the rules are binding. Such BCRs are to be drafted by the licensee, meet the requirements set up in the working papers adopted by the WP29 and submitted to the Lead Supervisory Authority for review and comments. Once the BCRs have been considered as final by all the Data Protection Authorities, the licensee shall request authorisation of transfers on the basis of the adopted rules by each national Data Protection Authority. The BCRs, inter alia, define the group members' global privacy policy with regard to the international transfers of personal data to those group members located in third countries that do not provide an adequate level of protection.

Concluding, in line with CJEU's jurisprudence[27], Article 45 Section 2 of the GDPR lays down the relevant criteria for an adequacy decision such as the third country's data protection legislation, implementation and supervision and its international commitments. Not all of the criteria have to be equally fulfilled, as an adequate level of data protection needs to be established by way of an overall assessment of the specific circumstances. In case of a positive outcome of such assessment, the European Commission may adopt an adequacy decision by way of an implementing act that shall provide for a mechanism of periodic review, specify its scope of application and, where applicable, the third country's Supervisory Authorities.

[26] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

[27] ECJ, ruling of 6 October 2015, Maximilian Schrems./Data Protection Commissioner, C-362/14.

10.3 Determining a Lead Supervisory Authority (LSA)

Since Operators are established in more than one EU/EEA Member State and consequently conducting cross border processing, Operators should identify the location of their main establishment, since the data protection authority within the said location shall be the competent authority to act as the Lead Supervisory Authority (LSA) for the purposes of Article 56 of the GDPR. For Operators whose main establishment is set in Malta, their LSA would be the IDPC.

The main establishment can be determined as either the place of its central administration in the Union, or else in the jurisdiction where decisions on the purposes and means of the processing of personal data are taken. In considering the latter, the establishment would need to have the power to have such decisions implemented in order to be able to be considered as the main establishment. Likewise, with regard to processors, the place of central administration shall be the processor's main establishment, however if the processor does not have a central administration, the establishment which carries out its main processing activities in the context of its activities shall be determined as the main establishment.

It is not unlikely that a licensee finds itself having two LSAs, in light of the fact that there could be two main establishments identified by the licensee as establishments wherein decisions on the purposes and means of the processing of personal data are taken. It is advised, however, that in such instances licensees categorise and identify the data processing being undertaken in each establishment, and hence the nature of the processing falling under the respective remits of the separate LSAs, so as not to have more than one LSA supervising the same set of data processing, thus nullifying the benefits ensued by the one-stop-shop mechanism. As stated by Article 29 Working Party[28] the GDPR does not permit "forum shopping": there must be an effective and real exercise of management activity in the member state identified as the organisation's main establishment. Organisations should be able to demonstrate to the LSA where decisions about data processing are actually taken and implemented, as they may be asked to prove their position. Furthermore, it should be noted that controllers without an establishment in the EU cannot benefit from the abovementioned one-stop-shop mechanism, but rather must deal with local supervisory authorities in every Member State they are active in, through their local representative.

11 Data Protection Officers

Every B2C gaming Operator must designate a DPO, since as a core activity, B2C Operators monitor individuals systematically and on a large scale. B2B Operators are not specifically required to appoint a DPO[29], but some may find it useful to do so on a voluntary basis.

Notably, it is highly likely than affiliates must also appoint a DPO, since here too, as a core activity, there is a possibility that the affiliate is monitoring individuals systematically and on a large scale.

[28] WP 29 Guidelines for identifying a controller or processor's lead supervisory authority, page 8.
[29] Unless such B2B operators also, as a core activity, monitor individuals systematically and on a large scale.

The role of the DPO may be held either by in-house employee, who knows the operational reality in which the processing take place and may also be outsourced, so long as he/she is designated on the basis of professional qualities, including expert knowledge of data protection law and practices, and the ability to fulfil the tasks laid down in Article 39 of the GDPR. A DPO may carry out more than one role within a controller's organisation, however, it is imperative that the individual designated as DPO is not simultaneously undertaking any role which could be deemed to be conflicting with that of a DPO, such as the role of an MLRO, HR development manager or marketing analyst. In any case, it is recommended to have a clear allocation of tasks within the DPO team, identifying only one natural person able to act as a point of contact with the data subjects and the Supervisory Authority.

A group of companies which are in possession of a corporate group licence[30] may appoint a single DPO provided that he/she is "easily accessible from each establishment[31]". The DPO must be easily accessible by data subjects and the respective supervisory authority, as well as internally within the organisation.

For example, an optimal solution of the fulfilment of "accessibility", required by Art. 37 par.2 of the GDPR could be represented by the usage of a multi-language telephone helpline or online portals, exclusively dedicated to privacy requests or complaints, if any.

It must be noted that DPOs are not themselves personally responsible in case of non-compliance with the GDPR, but it is the controller and/or the processor who is required to ensure and demonstrate that processing is being carried out in line with the GDPR. It must be noted that, DPOs and individuals carrying out DPO tasks are not allowed to be penalized or dismissed for their performance in executing the proper requirements of the GDPR.

In such cases, Articles 37-39 of the GDPR will become applicable to such organisation, as though the appointment of a DPO had been mandatory. Otherwise, such companies may opt to employ staff, or appoint external consultants, in order to handle data protection issues, without being themselves designated as a DPO. In fact, in such cases, it should be made clear that the title of such employee or consultant is not DPO.

For example, a good organisation that prevents conflicts of interests, could be represented by a privacy team composed by: (i) a Privacy Expert that monitors the compliance of the company with the GDPR, and who can report to the management, in case of major privacy issues; (ii) several Privacy Stewards within the relevant function/department that verify the correct use of the personal data and report to the Privacy Expert in case of issues relating to privacy. In any case, it is recommended to have a clear allocation of tasks within the privacy team.

[30] Either a corporate group licence issued by the Malta Gaming Authority, or one granted by another EU/EEA jurisdiction which affords equivalent safeguards and requirements.
[31] Article 37(2) GDPR.

Upon appointing a DPO, whether or not that DPO is an employee of the organisation, controllers/processors must ensure that the relevant DPO is given sufficient autonomy and resources to carry out the task effectively (e.g. budget on annual basis to improve technical and organisational measures and/or training modules on privacy matter related). It must also be noted that the DPO is bound by secrecy or confidentiality concerning the performance of his/her tasks.

In order to ensure that the DPO is accessible - whether internal or external - the DPOs contact details (i.e. information allowing data subjects and authorities to reach the DPO in an easy way) must always be available, and updated. Such details must also be communicated to the relevant supervisory authorities, and to the Malta Gaming Authority, and to the employees of the organisation. It is not necessary that the name of the DPO is communicated to the data subjects by virtue of publication on the gaming website, or within the gaming premises. It is up to the data controller or data processor to assess whether, depending on the specific circumstances, it may constitute useful or necessary information.

12 Accountability, Transparency and Good Governance

Operators are expected to establish comprehensive yet proportionate governance measures that take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of data subjects. This includes the implementation of appropriate data protection policies as well as appropriate staff training, and internal audits of processing activities. These measures are intended to minimise the risk of breaches and ensure the protection of personal data. Although most organisations already have good governance measures in place, these new requirements necessitate the review of these policies and the addition of new procedures as required.

Furthermore, in relation to the affiliates *status*, it is important to note that the review of conformity with GDPR of such gaming affiliates will become an obligation to be periodically performed. If an affiliate is not able to ensure privacy compliance, Operators will be obliged to either terminate the relationship with it or take the risk of potential liabilities, as explained in Section 6 above.

12.1 Data Mapping and Data Ledgers

The GDPR places an increased emphasis on proving compliance with data protection rules. Gaming Operators will be required to maintain a record of data processing activities, associated policies and procedures. Unless this is already in place, Operators should create and maintain a detailed inventory of personal data.

Without such an inventory, it is difficult for Operators to make informed choices on key strategic decisions relating to GDPR compliance.

The GDPR further requires that gaming affiliates commit to make available to the controller all information necessary to demonstrate compliance with its privacy obligations and allow for and contribute to audits, including inspections, conducted by the Operator or another auditor mandated by the Operator.

This obligation is reinforced by the need for gaming affiliates to keep a record of all categories of processing activities carried out on behalf of a controller. Therefore, a gaming affiliate that might process personal data on behalf of several Operators, shall keep a separate record of the categories of processing activities carried out by each of his Operators.

12.2 Data Protection Impact Assessments (DPIAs)

DPIAs constitute the process of systematically identifying potential privacy issues before they arise, to evaluate, in particular, the origin, nature, particularity and severity of that risk, and devise a way to mitigate it. This may also involve discussions with the relevant parties or stakeholders. This process may prove invaluable in determining the viability of future projects and initiatives, particularly with regards to new technologies.

Where a type of data processing is likely to result in a high risk for the rights and freedoms of individuals, the GDPR requires that the controller in question carries out a DPIA prior to the processing of the data, in order to assess the impact of the envisaged processing on the protection of the data. The IDPC will be publishing a list of risky processing in terms of Article 35(4) of the GDPR.

If a DPIA carried out by a controller indicates that an envisaged processing would result in a high risk in the absence of risk-mitigating measures taken by the controller, the controller shall consult the SA prior to the processing. The obligations to carry out DPIAs and consult with SAs in relation to high-risk processing operations directly apply to controllers only. But processors should assist controllers, where necessary and upon request, in complying with these obligations.

12.3 Adherence to Codes of Conduct

Codes of Conduct are a means for specific industry sectors, or groups of organisations, to create sector-specific rules on the processing of personal data to improve overall compliance with EU data protection law. Draft Codes of Conduct must be submitted to the IDPC, or any data protection supervisory authority, for formal approval. Such Codes represent an important component of broadening and adapting the tools for data protection compliance that controllers and processors can draw on, by way of a "*semi self-regulating*" mechanism.

Codes of Conduct not only help by providing guidance on specific compliance issues, but they also provide evidence of compliance with the GDPR and can be listed as a positive factor in a DPIA.

Non-EU/EEA organisations can adhere to approved Codes of Conduct as a lawful basis for cross-border data transfers. This may also simplify compliance obligations for organisations that frequently exchange data with other organisations in the same industry. Such adherence to Codes can demonstrate that non EU/EEA data importers (controllers as well as processors) have implemented adequate safeguards in order to permit transfers under Article 46 of the GDPR; transfers made on the basis of an approved code of conduct together with binding and enforceable commitments of the importer to apply appropriate safeguards may take place without any specific authorization from a supervisory authority and Codes may therefore offer an alternative mechanism for managing international transfers, standing on the same level as Standard Contractual Clauses.

Licensees are also encouraged to register for seal and certification schemes to obtain formal recognition of compliance with all, or a particular aspect, of EU data protection law. Guidelines will be issued by the WP29. That said, certification is voluntary. The competent supervisory authority will approve criteria for a common certification, the so called European Data Protection Seal.