Gambling Regulation and the General Data Protection Regulation (GDPR)

Information Note 2018

Introduction
On 25th May 2018, there will be new data protection legislation in force, both in Jersey and across the EU - the General Data Protection Regulation or GDPR.

GDPR is an evolution in data protection. It demands more of organisations in terms of accountability for their use of personal data, and adds to the existing rights of individuals. It creates an onus on companies to understand the risks that they create for others, and to ensure they are mitigating those risks.

Whilst this document does not constitute legal advice, it will assist gambling businesses by setting out some factors they should consider when assessing their processing of personal data. It also sets out our expectations on retention of information obtained for the purposes of fulfilling those obligations. It will remain licensees' responsibility to ensure they are legally compliant with GDPR and with our regulatory framework, and we recommend that operators obtain their own legal advice on compliance.

This document may be updated from time to time in accordance with legal developments.

General approach of the Commission to Compliance
Personal data processing

Processing of personal data will continue to be required in order to achieve compliance with a gambling licence. Providing facilities for gambling otherwise than in accordance with the terms and conditions of a licence is a criminal offence. It would also mean that operators' may be fined, and their licence could be revoked. We expect licensees to continue to be able to evidence that they have complied fully with their licence conditions.

We believe that because the JGC is a competent authority noted in Schedule 1 of the Data Protection (Jersey) Law 2018, implementing GDPR does not conflict with the requirements of gambling regulation. While GDPR enshrines the principle of consent, it is not the only basis on which to process personal data. Consent is one way to comply with GDPR, but the new law provides five other ways of processing data.

For processing to be lawful under GDPR, you need to identify at least one lawful basis before you start (though more than one basis may potentially apply) and consent will not always be the appropriate basis for data processing. For example, it is likely to be acceptable for personal data to be processed where a licence obligation requires it. This may be the case even where the need to process data in this way is not specifically set out by a licence condition, if the processing is realistically necessary in order to achieve the aim of the condition.

GDPR provides for a number of lawful circumstances which are designed to allow legitimate processing in circumstances where it may be not practical to acquire consent, and to ensure that public policy objectives (such as the reduction of problem gambling) are met. As well as consent, these include:

i. the processing is necessary for compliance with a legal obligation to which the controller is subject;
ii. processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
iii. the processing is necessary for the performance of a task carried out in the public interest
iv. the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data).

Licensees should note that more than one of the above bases may apply to some of the personal data they obtain (for instance, data obtained to ensure operators know their customers and can comply with Anti-Money Laundering obligations).

There are additional requirements where the personal data which is to be processed constitutes "special category" data, or data relating to criminal convictions and offences. We anticipate that the majority of data which licensees process for regulatory purposes (such as data on customer transactions) will not be special category data.

Licensees will wish to take steps to ensure they can demonstrate that, for each type of processing, they meet the relevant tests of the identified basis.

Data subject rights

GDPR gives data subjects certain qualified rights in relation to their data, such as the "right to erasure" and "the right to prevent decisions being made solely based on the automated processing of data". Data controllers should be aware of these rights, and make an assessment of the circumstances in which they do and do not apply. For example, such rights may not apply where their exercise conflicts with important regulatory objectives (such as the refusal of service to underage gamblers). Relevant considerations here may include:

i. The right to erasure is restricted where processing is still necessary in relation to one of the permitted purposes - for instance, compliance with a legal obligation, performance of a contract, or for the performance of a task carried out in the public interest.
ii. The right to prevent decisions being made solely based on the automated processing of data will not apply:

1. Where decisions are not made solely on this basis i.e. there is some human intervention
2. If the decision making is based on the data subject's explicit consent
3. If the decision is one which is authorised by law to which the controller is subject.

Licensees should also consider whether any other exemptions to data subject rights may apply. In particular, licensees should have regard to their role in preventing crime (including money laundering offences and cheating at gambling) and consider to what extent this objective would be likely to be prejudiced by a request to erase data or restrict processing of personal data, for example.

Other obligations
In addition to identifying a lawful basis for processing, operators will need to comply with other aspects of GDPR, such as any applicable requirements for transparency with data subjects, and safeguarding of personal data.

We do not anticipate that the need for such measures will cause a significant barrier to complying with gambling regulation. Indeed, being transparent with consumers at the outset (including informing them that their data may be passed to regulators when requested) may assist businesses to answer subsequent queries about the retention and use of their personal data for regulatory and public interest purposes.

Thorough consideration of transparency requirements will also assist data subjects, and assist data controllers to demonstrate compliance with obligations relating to accountability.

Next steps
We will not accept licensees simply stating that GDPR means that they are unable to comply with an aspect of gambling regulation, or otherwise take certain steps to protect the public interest.

Where genuine concerns, based on a careful and thorough analysis of GDPR and Commission regulation, are raised with us we will work with industry and where necessary, the Office of the Information Commissioner to resolve them. However, if an operator thinks that this might be the case, we would expect them first to have carefully considered all available legal bases and exemptions which may allow the specific activity. Documenting the consideration of the processing will assist in meeting requirements regarding accountability and documentation.

Whilst it will remain the responsibility of licensees to ensure they are legally compliant with GDPR, we are committed to offering assistance and support to help ensure that the licensing objectives and regulatory framework are upheld, and not prejudiced by the way operators interpret and implement compliance with their data protection obligations.

Retention of data
GDPR does not substantially alter the principles behind the development of policies for data retention. Licensees should already have assessed how long to retain data for, bearing in mind the legitimate purposes for which it was gathered and has been retained.

Under GDPR, data subjects may request that their personal data (including data which may be relevant to regulatory compliance) is erased. However, this right is not unrestricted.

In particular, such requests are unlikely to be valid if retention of the data is still necessary in relation to a lawful purpose. Where data which is relevant to a licensee's compliance with the regulatory regime has been obtained, licensees should have regard to the fact that we may wish to investigate whether a licensee has complied with their obligations. In some cases (for instance, where we are investigating a licensee's compliance with its social responsibility and anti-money laundering requirements as a result of a gambler stealing funds for gambling over a prolonged period of time), this may involve requesting account data which goes back a substantial period. Licensees should ensure that their retention policies ensure that such data will be available to the Commission if requested

Based on our experience of investigations to date, licensees should ensure that data which relates in any way to regulatory compliance should be available for a minimum period of five years after the end of a relationship with a customer.

Obtaining, retaining and using data for other social responsibility purposes

i. Licensees gather and retain personal information on customers in order to enable them to enter into and perform contracts, whilst taking into account their regulatory obligations. In common with other sectors we anticipate that licensees will continue to do so.

ii. Our licence conditions and codes of practice require operators, at the account opening stage and thereafter, to:

1. continue to obtain and retain information which is sufficient to satisfy them that underage gambling is not taking place;
2. continue to obtain and retain information to enable them to comply in relation to identification of problem gambling. Licensees are expected to continue to obtain and analyse data for the purposes of ensuring that their social responsibility policies and procedures are fit for purpose, taking into account currently available techniques for identifying and minimising problem gambling.

iii. Licensees should also consider to what extent data subject rights, such as the right to erasure and right not to be subject to automated decision-making, may not apply given the relevant lawful basis.

iv. Licensees should consider what retention period is necessary for any data which is obtained and processed for these purposes (whether also obtained for other purposes), noting that we may need to obtain such data even after an account has closed in order to establish whether or not a licensee has complied with its regulatory obligations.

Marketing to consumers

Licensees should ensure they are compliant with the law in relation to direct marketing.

Licensees should satisfy themselves that anyone they contract with in relation to direct marketing hold the appropriate consents from consumers for marketing of the licensees' products. Ongoing failure to ensure compliance may result in regulatory action.

Example licence conditions and codes of practice which necessitate the obtaining, processing and retention of personal data

Socially Responsible Gambling

Licensees must have and put into effect policies and procedures intended to promote socially responsible gambling, including Self-Exclusion.
Licensees must, as soon as practicable, take all reasonable steps to prevent any marketing material being sent to a self-excluded customer.

Licensees must put into effect procedures designed to ensure that an individual who has self-excluded cannot gain access to gambling. These procedures must include a register of those excluded with appropriate records.

Anti-Money Laundering

Licensees must conduct an assessment of the risks of their business being used for money laundering and terrorist financing. Such risk assessment must be appropriate and must be reviewed as necessary in the light of any changes of circumstances, including the introduction of new products or technology, new methods of payment by customers, changes in the customer demographic, or any other material changes, and in any event reviewed at least annually.

Licensees must ensure they have appropriate policies, procedures and controls to prevent money laundering and terrorist financing.

Licensees must ensure that such policies, procedures and controls are implemented effectively, kept under review, revised appropriately to ensure that they remain effective, and take into account any applicable learning or guidelines published by the Jersey Gambling Commission or the Jersey Financial Services Commission.

Problem gambling

Licensees must put into effect policies and procedures for customer interaction where they have concerns that a customer's behaviour may indicate problem gambling.

Reporting suspicion of offences

Licensees must as soon as reasonably practicable provide the Commission or ensure that the Commission is provided with any information that they know relates to or suspect may relate to the commission of an offence under the Law, including an offence resulting from a breach of a licence condition or a code provision having the effect of a licence condition.

Information provision

Licensees are required to provide the Commission on request with such information as the Commission may require about the use made of facilities provided in accordance with the licence, including the licensee's policies in relation to, and experiences of, problem gambling.

Technical standards
Licensees must comply with the Commission's technical standards and with requirements set by the Commission relating to the timing and procedures for testing. For example, measures intended to deter, prevent, and detect collusion and cheating. Gambling systems must retain a record of relevant activities to facilitate investigation and be capable of suspending or disabling player accounts or player sessions. Operators must monitor the effectiveness of their policies and procedures.