Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

The Information Commissioner's response to the Department for Communities consultation on the proposed/draft Gambling Codes of Practice

Introduction

1. The Information Commissioner (the Commissioner) is pleased to respond to the Department for Communities (DfC) consultation in relation to the introduction of a Code of Practice for gambling operators in Northern Ireland under Clause 15 of the Betting, Gaming, Lotteries and Amusements (Amendment) Bill.

2. The Information Commissioner's role includes the regulation of the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000 (FOIA), among other pieces of legislation. Given our role as a regulator, it would not be appropriate for us to respond with a view on the different questions and options proposed within the consultation document. However, there are data protection and information governance implications in the proposals which we have raised below for your consideration.

3. The proposed Code of Practice (the Code) is understood to apply to all facilities in which gambling is made available to the public, encompassing both destination-based venues and online services. For the purpose of the Code, the term "gambling" relates to betting, gaming or the participation in a lottery (with the exception of the National Lottery). We therefore recognise that there will be inevitable differences in the application of the data protection legislation among the respective controllers due to their operating environment and the service they offer. Consequently, we will aim to reflect this in our comments and guidance below.

Preparation of a legislative or regulatory measure

4. Given the statutory nature of the proposals, it is important to first draw your attention to Article 36(4) of the UK GDPR which requires government departments and other public sector bodies to consult with the ICO on policy proposals for legislative or statutory measures relating to the processing of personal data. As your policy proposals are in relation to a power proposed under Clause 15 of the Betting, Gaming, Lotteries and Amusements (Amendment) Bill, this will trigger the need for consultation with us under Article 36(4).

5. To effectively meet the principles of this requirement it is important that early engagement is undertaken during the formative stages of the development of policy proposals to meet the spirit of this requirement.

6. The DCMS guidance on the consultation process under Article 36(4) is available here, alongside the Article 36(4) Enquiry Form which will need to be submitted to our legislation consultation mailbox: legcon@ico.org.uk. Your Departmental Data Protection Officer will be able to guide you through the process.

7. We will often ask to view your data protection impact assessment (DPIA) regarding the legislation, as this can form an integral part of the consultation we carry out. Please note that the DPIA published as part of the consultation documentation would not suffice in this regard as it is a DPIA specifically on the consultation exercise, rather than an assessment of the personal data implications of your policy proposals.

8. In the meantime, below we have briefly set out a few key data protection considerations pertaining to the current consultation documentation.

DPIA

9. The draft Code of Practice contain proposals which necessitate the requirement for certain controllers within scope to undertake a Data Protection Impact Assessment (DPIA). We therefore recommend that you ensure that the relevant controllers are aware of the following:

10. Article 35(1) of the UK GDPR states that a DPIA should be carried out by the controller where proposals are likely to result in a high risk to the rights and freedoms of individuals. The DPIA should consider the measures, safeguards and mechanisms envisaged for mitigating those risks to ensure the protection of personal data and thus compliance with Data protection law.

11. One of the criteria which necessitates a DPIA includes "*the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children*". It is important to note that a child is anyone under the age of 18

years.

12. Information Society Services (ISS) are online services that provide online products and services (including apps, programs, websites, games or community environments and connected toys and devices with or without a screen. Providers of ISS will also be required to complete a DPIA if a child is likely to access their service. This remains the case when the service is not inherently directed towards children. Online providers should however note that they may also trigger several other criteria indicting the need for a DPIA, including large-scale profiling, biometric data and online tracking. Further guidance regarding DPIAs and the processing of children's data can be found here.

13. Whilst we note that the Code predominately relates to the processing of customer data over the age of 18 years, some products (such as lotteries) are open to children over the age of 16 years. It is therefore important that online providers are aware that they will need to complete a DPIA if children are likely to access their services.

14. The ICO therefore recommends that the DfC reference this obligation in the Code of Practice and further advises controllers to consult the ICO's DPIA guidance on this matter as a priority. However, depending on the services offered and the intended customers, it will be for controllers to decide whether the threshold of requiring a DPIA is reached and record their rationale either way. Further information on DPIAs, including the obligation to consult the ICO in certain cases, is available here.

Personal data processing activities for different types of providers

15. The ICO has noted that the drafted Code of Practice primarily focuses on the standards and safeguarding measures for destination-based venues as opposed to online service providers. The Code should consider how the personal data processing activities may differ depending on whether a physical or online service has been engaged. This may include considering whether the proposed measures are likely to be adequate, necessary and proportionate to the specific risks and trends seen in the relevant environment, and also whether the Code should consider potential differences in relation to the collection of data, retention periods and security mechanisms.

Protection of children and young people

The ICO's Age Appropriate Design Code

16. DfC's draft Code indicates that in some instances online gambling providers will allow access to children aged 16 years and older (for example, providers of lotteries). It is the ICO's view that the Code should explicitly inform controllers who offer online services to children, or if their online service is likely to be accessed by children, that they must comply with the ICO's statutory Age Appropriate Design Code (AADC).

17. The ICO's AADC has 15 standards that ISS must conform with, including undertaking a DPIA, providing transparency information that can be understood by users, having age appropriate application and not sharing children's data unless there is a compelling reason.

Age assurance techniques

18. The Code references the protection of children and young people and in turn covers steps to ensure that persons under the relevant legal age (whether that be 16 for lotteries or 18 for other gambling products) do not access products or services prohibited to them by law. For destination-based venues this includes requesting photographic evidence on an ad hoc basis under the 'Think 18' and 'Think 21' principles. It is the ICO's view that the Code should also detail how online providers should verify their customer's age. However we note that the Code of practice states that *"Lotteries must operate age verification procedures for all persons",* nonetheless the instructions regarding this process are not explicitly clear. More detail should be provided about this process.

19. Providers of services which are not intended to be accessed by audiences under the age of 18 years (ie betting or gambling facilities) should consider age assurance techniques which allow controllers to ascertain a **high level of certainty** of age assurance. This will ensure that risks to children are mitigated and access to the service is prohibited.

20. Providers who offer services accessible to over 16 year olds should also consider robust age assurance techniques to ensure that the user is of the appropriate legal age to participate in their chosen activity. The proposed age assurance techniques should consider

the range of the audience and the needs of customers at different ages and stages of development.

21. It may be important to note as a 16-year-old is approaching adulthood and will not enjoy the same rights and freedoms of an individual 18 years old or above, it is unlikely that these customers will have access to a number of photographic identification documentation referred to in the Code. It is therefore essential that the DfC has balanced the need to safeguard younger customers from inappropriately accessing age restricted products against Principle A of the data protection principles, specifically the 'fairness' criteria. The DfC should also record its decision making process in relation to this matter. In respect to this matter you may find it useful to refer to the Information Commissioner's Opinion regarding Age Assurance for the Children's Code (AACC).

Retention of age assurance information

22. As explained in the section above, some customers will be required to provide documentary evidence to controllers in order to access the relevant products or services. This includes online services. It is unclear from the Code whether controllers are expected, or required, to retain evidence or information to demonstrate that they have complied with the age verification process. It is recommended that DfC consider how controllers may best comply with their obligations under data minimisation, taking into consideration the types of facilities as well as the age of customers, covered in this code.

Purpose limitation

23. When deliberating on age assurance techniques, controllers should consider their compliance with the purpose limitation principle. The purpose limitation principle means a controller can only use the personal data for the purposes for which it was collected for. Personal data should only be processed for a new purpose if either it is compatible with its original purpose, consent from the data subject is obtained or you have a clear obligation or function set out in law.

24. Therefore, should controllers wish to process the personal data they obtained during the age assurance process for other purposes (ie to determine whether an individual can be placed on a marketing list) then they will need to assess whether the purposes

are comparable. Furthermore, controllers will be obliged to inform their customers of the purpose(s) for processing and consequently the Code should high light this obligation under the right to be informed.

Customer care – affordability check

25. The proposed Code of Practice articulates that a customer will be required to undergo an 'affordability check' to continue gambling once a 'trigger' limit has been met. The customer will only be obliged to obtain one positive affordability check in a 12 month period and will be able to provide this information to several service providers to demonstrate their suitability to exceed the limit. Before the implementation of this practice DfC must consider its compliance with the Data Protection law in relation to the proposed affordability check.

Lawfulness

26. To comply with the lawfulness element of principle A, organisations implementing the affordability check will need to consider their lawful basis for processing under Article 6 of the UK GDPR prior to the commencement of processing.

27. More so, when carrying out an affordability check controllers should be mindful of the language used and ensure that their customer understands that there is a difference between consenting to the affordability check and consent as a lawful basis for processing. This will be essential to manage the customers' expectations and to better understand their wider personal information rights.

Fairness

28. To further compliance with the fairness component of principle A it would be beneficial for the DfC to provide further guidance to controllers regarding the type of credit check required to facilitate the affordability check. This is because there are two types of credit searches which have different effects on data subjects.

29. A soft check is an initial look at certain information on a credit report and is often utilised to decide how successful an application would be without performing a full assessment of the individual's credit history. These checks are only visible to the organisation completing the check and the customer. Consequently, they have no impact on the credit score.

30. In contrast, a hard check involves a complete search of a customer's credit history and will be recorded on their credit report. This type of check can have adverse affects on the customer, especially if a number of hard credit checks are carried out over a short period of time and in turn can reduce the individuals ability to secure credit in the future.

31. Consideration should also be given as to whether the DfC should specify which Credit Reference Agency's (CRA's) should be utilised when executing the credit check. This is because CRA's may use a variety of methods to calculate an individual's credit score and their financial standings. Should controllers use different CRA's, then the DfC should determine whether an individual could receive different outcomes from different controllers based on their chosen CRA.

32. It is therefore important for the DfC to consider which type of credit search is necessary and proportionate in relation to the affordability check as well as the chosen CRA's and whether there could be any disproportionate effects on customer's rights and freedoms. This information must also be provided to the customers in their privacy policy and/or notice to ensure that the controller is transparent about their processing.

Transparency

33. Under the transparency aspect of principle A, controllers must be transparent about how they will use and process personal data, and individuals have a right to be informed by controllers about what will happen to their data. It may therefore be beneficial for the DfC to remind those executing the affordability check of this fundamental right, and signpost them to our guidance on the right to be informed.

Adequacy of processing

34. It is vital that the DfC considers whether the processing activities undertaken during the affordability check is adequate in relation to the specific problems that you are seeking to address.

35. When considering the adequacy of the proposed processing activities you may find it beneficial to refer to our work with the House of Lords (HoL) Gambling Industry Select Committee (the Committee). The Committee recommended that the ICO works with the Gambling Commission, the Betting and Gambling Council and UK Finance, to resolve perceived data protection barriers to sharing personal data in order to protect customers from harm related to gambling. Please note that we are committed to continuing our work in this area. Further information on this matter can be found in our letter to the Committee here as well as the evidence we provided to the Select Committee (pages 617-619) as part of their inquiry into the social and economic impact of the gambling industry.

36. This work has explored the suggestion for a Single Customer View (SCV) that would standardise data points about a customer which are collected by operators, measured against an industry-agreed standardised risk score, to produce an accurate, real time assessment of whether a customer is at risk of harm. This proposed approach would utilise data already routinely processed by operators when managing relationships with their online customers.

37. It would therefore be beneficial for the DfC to consider whether their safeguarding goals are likely to be successful with the implementation of annual affordability checks, how the proposals compare to a project like the SCV and whether the approach is suitable for physical venues and online settings alike. In the event that the DfC believes that their goals could be undermined by any part of the processing then the proposal should be reassessed

Necessity and proportionality

38. The ICO would like to recommend that the DfC should consider and document the necessity and proportionality of the affordability check proposals. In doing so you may wish to articulate why the proposed affordability check is the most suitable initiative, taking into consideration the goals of the Code.

Accuracy

39. It is important that appropriate thought is given to the accuracy principle under Article 5(1)(d) of the UK GDPR. This principle stipulates that personal data shall be accurate, and where necessary, kept up to date. In this instance DfC should whether annual affordability checks help to facilitate compliance with the accuracy principle. In the event that the affordability check could be interpreted as inaccurate or misleading as to a matter of fact (ie indicate that a customer is suitable to exceed the trigger limit when they are in fact unsuitable) then you must reconsider this process.

The rights of data subjects

40. It would be beneficial for the DfC to consider how controllers will comply with the rights of data subjects and ensure that the application of these rights are articulated in the controller's privacy information or notices.

41. Particular consideration should be given to the right to object to processing. As this is not an absolute right the controller (with the exception of processing in relation to direct marketing) will be required to take into account the lawful basis for processing to determine whether or not to uphold the request. The processing can continue if there is a compelling justification which overrides the individuals interest. All requests of this nature need to be considered on a case-by-case basis.

42. Furthermore, Article 22 of the UK GDPR limits the circumstances in which controllers can make solely automated decisions (ie with no human involvement in the decision-making process), including those based on profiling, that have a legal or similarly significant effect on individuals. This type of decision-making can only be carried out where the decision is necessary for the entry into or performance of a contract, authorised by domestic law applicable to the controller, or based on the individual's explicit consent. In addition, if special category data is processed, organisations can only carry out the processing described in Article 22 (1) with the individual's explicit consent, or where the processing is necessary for reasons of substantial public interest.

Upholding information rights

3rd Floor, 14 Cromac Place, Belfast, BT7 2JB
Tel. 0303 123 1114
www.ico.org.uk

Privacy and Electronic Communications Regulations 2003 (PECR)

43. We note that the proposed draft provides guidance regarding the marketing of customers. It is important to note that consideration should be given to the application of PECR. For further information with respect to the PECR regulations please see our guidance here.

With the consideration of the information above, we now expect you to consult with the ICO formally under Article 36(4) of the UK GDPR. During the consultation process we will provide further detail in relation to the points mentioned above.

I hope this is of use to you but if you have any further queries please do let me know.

Yours sincerely,

Ceri Hall
Senior Policy Officer – Northern Ireland
Information Commissioner's Office