SUBMISSION TO THE INFORMATION COMMISIONER

–

REQUEST FOR AN INVESTIGATION INTO THE ONLINE GAMBLING INDUSTRY:

Sky Betting and Gaming and related third parties

A. Introduction and purpose of this submission

I. Background

1. This submission is provided to the Commissioner on behalf of Clean Up Gambling as a detailed, reasoned and evidenced basis upon which the Commissioner should commence an investigation, using the applicable regulatory powers, into the processing of personal data by the online gambling industry. In particular, this submission sets out why that investigation should usefully start with the Sky Betting and Gaming group of platforms[1] ("**SBG**"), as a proportionate and instructive 'way in' to this particular data ecosystem. Clean Up Gambling is not a data subject; it cannot make a complaint under section 165 of the Data Protection Act 2018. Nonetheless, the Commissioner has the general task of monitoring and enforcing the UK GDPR in Article 57(1)(a), and of conducting investigations on the application of the UK GDPR in the absence of a data subject complaint in Article 57(1)(h). This submission formally invites the Commissioner to exercise his discretion to commence such an investigation.

2. This submission highlights concerns about data processing in the online gambling industry, as were first comprehensively documented in an expert report published in January 2022, titled *Digital Profiling in the Online Gambling Industry* (referred to as the '**Report**' herein). The Report was commissioned by Clean Up Gambling and written by Cracked Labs, an independent research institute

[1] As this submission details, SBG is not an identifiable corporate entity but, confusingly, appears to be a trading name related to a number of different companies. We use SBG as this matches the way that the group refers to itself in parts of its privacy notice.

specialising in information technology. The Report contains a detailed and forensic investigation into the practices of one major online gambling group, Sky Betting and Gaming, which is part of the Flutter group, the largest provider of online gambling in the UK.[2] A copy of the Report is enclosed with this submission.

3. The Report focuses on SBG's behavioural profiling of data subjects which involves extensive processing of personal data, including special category data and other sensitive information, by SBG and third-party companies. The Report was limited to analysing subject access request responses alongside what could be observed in users' browsers. Its authors were unable to observe the internal data practices of SBG or the third parties. Despite those limitations, the Report was able to show that data subjects cannot know the full extent of processing conducted by SBG nor understand the consequences of the profiling, such that the processing is "*invisible*". Nor is it possible to know all the entities that process individuals' personal data. Indeed, despite its technical expertise and extensive investigations, even Cracked Labs was unable to determine the full extent of the profiling.

4. Furthermore, SBG's processing is unfair. The method of profiling, approach to processing and absence of transparency exemplifies 'dark pattern' practices. Those dark patterns have real-world consequences for data subjects. For instance, the processing cannot be within data subjects' reasonable expectations, data subjects are unable to effectively exercise their rights and SBG's extensive behavioural profiling, which seeks to maximise the time and money users spend gambling, can be used to exploit the vulnerabilities of individuals at risk of developing clinical addictions.

5. The gravity of the problems identified in the Report is intensified by its scope and scale. The lack of a lawful basis for the deployment of tracking technology, coupled with the flawed approach to consent for the profiling that follows, has led to a widespread and systemic problem within SBG. That problem has developed over decades, meaning the controller has processed data unlawfully on a vast

[2] https://www.bettingoffers.org.uk/articles/biggest-betting-companies-in-the-uk/

number of individuals. Those problems reflect an endemic of unlawful processing by the online gambling industry.

II. Scope of submissions and structure

6. This submission provides an overview of the Report, then highlights the tension between the profiling and data processing practices of SBG and the UK GDPR. The submission is structured as follows:

   6.1. The submission first addresses Clean Up Gambling and its work on data processing in the online gambling industry (paras 13 to 14).

   6.2. We then provide some background about online gambling (paras 15 to 18).

   6.3. The submission then provides an overview of the Report (paras 19 to 21).

   6.4. The submission then analyses the legality of the data processing conducted by SBG (para 22 to 134).

   6.5. The submission concludes with the request that the Commissioner exercise his powers under the Data Protection Act 2018 ("**the DPA**") and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**") to investigate and to take formal regulatory action (paras 135 – 146).

III. Scope of action required

7. The breadth of data processing uncovered in the Report is alarming. The Report demonstrates that it is impossible for data subjects to meaningfully understand how their data is used and the profiling they are subjected to. Ordinary data subjects cannot hope to understand how their data is being used, even to the extent shown by the Report, let alone considering hidden processing within gambling companies, profilers, and data brokers. Such profiling practices are in fact routine across the online gambling industry; a problem that the Information Commissioner must address.

8. Action is required from the only relevant regulatory body, in the form of the Commissioner, to protect individual data subjects from an industry that has

grown accustomed to profiting from invasive and invisible processing of individuals' personal data.

IV. Summary

9. The Report identifies, in summary, the following concerns for compliance with the data protection regime:

   9.1. **Legal bases** – SBG purport to rely on consent for the profiling and behavioural analysis set out in the Report. However, such reliance on consent is misplaced. SBG do not provide sufficient information for a data subject to make an informed decision. Moreover, SBG do not allow individuals an option to opt out from such profiling. Any such reliance on consent is therefore invalid.

   9.2. **Deployment of cookies and similar technology** – SBG deploy cookies and similar tracking technology, without seeking consent from users. Users are instead presented with a binary "accept" box to the deployment of such technology, contrary to the requirements of Regulation 6 of PECR.

   9.3. **Transparency notices** – SBG's privacy notices are defective and do not provide sufficient information for a data subject to know what data is being processed, its source and recipients or how to exercise rights over that data.

   9.4. **Data subject rights** – The failure to be transparent with how personal data is being processed and the dark patterns used by SBG has consequent effects for the ability of data subjects to exercise their rights.

   9.5. **Retention periods** – SBG retain all behavioural data, indefinitely. The Report shows that data on all interactions with SBG platforms was retained for over a decade, without any basis.

10. Thus, Clean Up Gambling seeks a full investigation into (a) the processing conducted by SBG (and the related group of companies), (b) the processing by third-party companies used by SBG, (c) the further processing by third parties facilitated by SBG and (d) in the light of the results of that investigation, any

necessary further action by the Information Commissioner that will protect individuals from the continuing widescale and systematic infringements of their rights afforded under the data protection legislation.

V. Concerns about the wider industry

11. The problems relating to SBG are illustrative of systemic issues within the industry. Those problems reflect an entrenched and covert approach to widescale profiling by the online gambling industry. This is an industry which, as the Report highlights, is increasingly reliant on gathering significant amounts of personal data and exploiting that data to target their services and to maximise profit, with scant regard to their obligations under data protection laws and the rights or welfare of data subjects. For this and the further reasons detailed in this submission, it is imperative that the Information Commissioner not only investigates the companies highlighted in the Report but also acts in respect of other relevant actors that operate in the online gambling industry, whether the licenced operators themselves or the third parties on which they rely.

12. The Commissioner should act to ensure that the industry operates consistently with the data protection framework. In the absence of action by the Commissioner to remedy non-compliance, data subjects will be left without the protection that the data protection framework was designed to provide, to the significant detriment of their finances and even their health. The risks and widespread nature of gambling addition are well-known and stands this context apart from other sectoral investigation work the Commissioner has undertaken; data broking and AdTech are industries with serious compliance problems, but they are very unlikely to result in processing intended to keep vulnerable people gambling, driving some ultimately to suicide. We request the Information Commissioner's Office to exercise its powers, commencing with an audit of online gambling companies, as well as the profiling companies and data brokers whose services they use. Such an audit is required before such companies are afforded greater access to data, following the proposed introduction of the "Single Customer View".

B. Clean Up Gambling

13. *Clean Up Gambling* is a not-for-profit campaign by *AMZC Ltd*, supported by grant-funding from Derek Webb, who founded and funded the *Campaign for Fairer Gambling*. *Clean Up Gambling* is run by Matt Zarb-Cousin, who spearheaded the *Campaign for Fairer Gambling* during the period in which it lobbied successfully for a reduction in the maximum stake on Fixed Odds Betting Terminals from £100 to £2 a spin.

14. As part of the focus on making gambling fair, Clean Up Gambling have taken the leading role in uncovering abuses of personal data within the online gambling industry. This includes submissions to various government bodies concerning the scale of profiling and the proliferation of use of third-party behavioural analysis companies. Clean Up Gambling's work on data misuse in the online gambling industry has featured in several press publications, including featuring in BBC documentaries.[3] It is a specialist, reputable and expert campaigning organisation acting in the public interest.

C. Background

15. The Report details the proliferation of online gambling – and the related increase in gathering and processing of personal data by licenced operators to monitor individuals, profile them, and tailor interventions to those profiles so as to maximise the amount of money extracted from individuals.

16. The licenced operators are not transparent about such practices. The Report highlights the significant discrepancies between the information provided to users and the realities of SBG's data processing activities.

17. SBG works with a network of third-party profiling companies and data brokers to carry out at least four distinct but related processing operations. The Report details how SBG conduct detailed profiling with Signal Inc. Following the publication of the Report, Signal Inc stopped operations in the UK. Clean Up Gambling understand that, rather than cease profiling or increase transparency,

[3] https://www.bbc.co.uk/programmes/m0010l43 at 36m - 40m

SBG has instead replaced Signal's profiling services with another company: Tealium - https://tealium.com/. The Report highlights that those invasive processing operations occur in respect of both anonymous visitors to its websites and users that sign-up to its platforms:

17.1. SBG records and stores data about the actions visitors and users take on its websites.

17.2. Pseudonymous identifiers are created, stored and retrieved on individuals' browsers using monitoring technology (often through "*cookies*"). The identifiers track individuals who visit SBG's websites, but also websites of other clients of SBG's profiling providers. The identifiers are used to facilitate the transmission of information about individuals' browsing and other behavioural activity from SBG's sites to a range of third parties, both directly and indirectly.

17.3. SBG and associated profiling companies use email addresses or pseudonymous identifiers derived from them (such as via hashing and 'hashed email addresses') to identify individuals and facilitate further collection of personal data (marketing email open rates, for example).

17.4. The data collected through the means described at 17.1 to 17.3 are used by both SBG and related third-party profiling companies to build profiles on individuals. These profiles include individuals' browsing and gaming history, are enriched with other demographic data, and are used to generate inferences such as an individual's preferred game, how influenced they are by certain messaging and likely value to SBG if they can be attracted back to one of its websites.

18. The use of personal data by the online gaming industry is of public concern. Indeed, the international press[4] has highlighted the way UK operators have

[4] Adam Satariano, New York Times, *What a Gambling App Knows About You* (24 March 2021). See also, https://www.bbc.co.uk/news/technology-56580411; https://techcrunch.com/2022/02/04/on-metas-regulatory-headwinds-and-adtechs-privacy-reckoning/; and https://www.thisismoney.co.uk/money/markets/article-10444901/Suicidal-gambling-addict-groomed-Sky-Bet-hooked.html

processed data and profiled individuals, warning against the introduction of such practices elsewhere.

D. The Report

19. Clean Up Gambling instructed Cracked Labs to carry out the most detailed investigation into data flows in the online gambling industry to date. The investigation lays out the scale and depth of behavioural surveillance and profiling used by online gambling operators. It details the network of third-party companies that receive data on anonymous visitors and registered users to SBG's websites and build detailed and intimate profiles of them, often without their knowledge. Such profiles include indicators of personal vulnerability and addictive behaviours, which can then be used to target the most vulnerable. Such targeted messaging needs to be seen in the context of the human impact of online gambling, where:

> *"The gambling industry spends £1.5 billion a year on advertising, and 60% of its profits come from the 5% who are already problem gamblers, or are at risk of becoming so."*[5]

20. In particular, the investigation shows:

20.1. **The online gambling industry processes vast quantities of personal data of a highly sensitive nature** – The investigation shows that gambling platforms do not operate in a silo. Rather, gambling platforms operate in conjunction with a wider network of third parties. The investigation shows that even limited browsing of 37 visits to gambling websites led to 2,154 data transmissions to 83 domains controlled by 44 different companies that range from well-known platforms like Facebook and Google to lesser-known surveillance technology companies like Signal and Iovation, enabling these actors to embed imperceptible monitoring software during a user's browsing experience. The investigation further shows that a number of these third-party companies receive behavioural data from gambling

[5] Select Committee on the Social and Economic Impact of the Gambling Industry *Gambling Harm—Time for Action* Report of Session 2019-21 - published 2 July 2020 - HL Paper 79.

platforms in real-time, including information on how often individuals gambled, how much they were spending, and their value to the company if they returned to gambling after lapsing.

20.2. **Lack of transparency** – Both online gambling operators and third parties were asked to provide access to the data they were processing on individual consumers to understand how that information was being used. The investigation explains how the companies responded to those requests, finding that (i) the companies were not transparent about what data would be collected and (ii) did not disclose all data being processed, contrary to Article 15 UK GDPR. That lack of transparency makes it difficult for individuals to know what is happening with information being held about them and impairs the ability of individuals to exercise their rights.

20.3. **Potential to exploit vulnerable individuals through behavioural profiling** – Gambling disorders are characterised by repetitive traits that signal a form of addictive behaviour. The potential to exploit such traits is extremely lucrative to gambling platforms. Being able to know what individuals are playing and how to ensure continued engagement has become a reality through behavioural profiling. The Report shows that such behavioural profiles are being created by the industry. For example, a request for access to personal information was made to Signal, a profiling company owned by the credit reporting giant TransUnion. In response, Signal disclosed detailed personal profiles revealing intimate gambling behaviour. The files contained 186 separate attributes for a single individual. Those 186 attributes painted a detailed and personal portrait of the individual's gambling behaviour, including their propensity to gamble, their favourite games, and their susceptibility to marketing. The profiles also included metrics as to how much they are worth financially to the gambling companies and categorised individuals on their inferred "value" to operators. Additionally, the investigation found that these data profiles were able to determine whether individuals have self-excluded from gambling or not. The Commissioner will be able to contrast the nature of these attributes, their basis in granular and real-world data about the individual,

and the use made of this profiling (including the direct interest in the profiling at the individual data subject level), with that considered in detail in the context of the Enforcement Notice issued against Experian, and the subsequent appeal proceedings.

21. These practices as uncovered in the Report are inconsistent with the DPA 2018, UK GDPR and PECR.

E. Legal Framework and Concerns – Breaches of the DPA 2018, UK GDPR and PECR

22. While the Report is limited to investigating data processing at the user level, without being able to access the data processing within the platforms themselves, the Report suggests that SBG's processing activities – and that of its third-party partners – involve breaches of the DPA, the UK GDPR and PECR.

23. This submission is structured around nine primary concerns about the data processing by SBG, as revealed by the limited information that is available to Clean Up Gambling:

    23.1. Identity of the controller(s)

    23.2. Legal bases for processing

    23.3. Special category data

    23.4. PECR breaches

    23.5. Transparency of processing activities

    23.6. Retention periods

    23.7. Data subjects' rights

    23.8. Purpose limitation

    23.9. Dark patterns and unfair processing

24. We address the concerns in turn.

I. Identity of the data controller

Background

25. SBG does not exist as a customer-facing entity; it does not have a website nor are there other means by which an individual can interact with it. Rather, SBG is described as an umbrella company, with three subsidiary companies, which each have multiple brands. SBG describe this organisation as follows:[6]

> *'Sky Betting and Gaming' means companies within the Sky Betting and Gaming Group: Bonne Terre Limited (whose trading names include Sky Bet, Sky Vegas, Sky Casino, Sky Bingo and Sky Poker), Hestview Limited (whose trading names include Sky Games, Sky Sports Super 6, Sky Sports Fantasy Football, Fantasy Six a Side and Sportinglife) & Core Gaming Limited.*

26. However, SBG's Cookies Policy and Privacy Notice (the "**Notice**" herein) states that "*Our Policy explains how Sky Betting and Gaming uses your personal data*". The SBG Privacy Notice further states that: "*Sky Betting and Gaming handles your personal information*".

27. Thus, "*Sky Betting & Gaming*" is said to "*handle*" and "*use*" data, yet SBG does not exist as a single entity. SBG are also said to be part of the "*Stars Group*" of companies, and the Notice variously refers to processing conducted by entities within the Stars Group. For instance, the relevant section on marketing refers to marketing by the Stars Group (rather than SBG).

28. The Stars group of companies are then said to operate under The Flutter Group, which includes other gaming platforms, described as follows:

> *The companies listed within the previous paragraph are wholly owned by Flutter Entertainment Plc. Any reference to "The Flutter Group" within this Privacy Policy includes Flutter Entertainment Plc and all or any of its direct or indirect subsidiary undertakings, joint venture partners, and their related companies wherever located in the world as may exist from time to time*

[6] https://support.skybet.com/s/article/Cookies-Policy-Privacy-Notice#header289

including, but not limited to, Paddy Power, Betfair, Timeform, Sportsbet, BetEasy, FanDuel, TVG, Adjarabet, Sky Betting and Gaming, Full Tilt, PokerStars and FOX Bet. […]

This means that whichever of our products and services you use in any country in which we operate, we may share your personal information among all the companies in The Flutter Group for any of the purposes outlined in this policy.

29. The Notice however goes on to state that:

In the UK, to comply with local data protection law, Hestview Limited, Bonne Terre Limited & Core Gaming Limited are registered as 'Data Controllers' with the Information Commissioner's Office ("ICO") and details are published on a public register on the ICO website at ***http://ico.org.uk*****.**

The Stars Group Inc. operates its UK operations through Stars Interactive Limited ("Stars Interactive") which maintains a separate privacy policy. Stars Interactive is registered as a Data Controllers with the Isle of Man Information Commissioner and details are published on the public register at ***https://www.inforights.im***

30. There are accordingly various companies involved in the data processing activities of concern. Only some of those entities are registered with the ICO. It is not clear on the face of the information in the Notice what entity or entities act(s) as the data controller(s) when an individual visits or uses the SBG platforms, nor is the data processing relationship between these entities clear. This impairs the ability of data subjects to understand who processes their data, for what purposes or how to exercise their rights. Particularly given the issues arising from the substantive processing considered below, there is at the least a serious risk that the published information is deliberately obscuring and confusing the identity of the relevant controller, so as to reduce the risk of data subjects and regulators being able to investigate effectively.

Who are the controllers?

31. Data subjects cannot know who is controlling their data based on the information provided in the Notice, for the following reasons:

31.1. A data subject will interact with one of the SBG brands, such as Sky Bet, Sky Vegas, Sky Casino, Sky Bingo or Sky Poker. None of those brands are named as data controllers.

31.2. A data subject is told that the Notice applies to SBG and that "*Sky Betting and Gaming handles your personal information*". However, SBG has no corporate identity. The statement is thus meaningless.

31.3. SBG is not registered with the ICO.

31.4. Rather, the relevant registration with the ICO is for "*Bonne Terre Limited*" (registration number ZA074790), which lists "*other names*" for six other companies, including SBG.

31.5. Stars Interactive Limited is registered with the Isle of Man information commissioner.

31.6. Flutter UK is listed with the ICO as "*Hestview Limited*" (registration number Z8579708).

31.7. Core Gaming Limited is not registered with the ICO, contrary to the Notice.

32. The information provided about SBG's corporate structure in the Notice is unclear, obscuring the identity of the entity or entities responsible for compliance with data protection law.

33. Data subjects are presented with a further layer of uncertainty as to the identity of the data controller as different corporate entities are listed for licencing purposes than those registered with the ICO. The Notice states (sic):

> *Flutter Entertainment Plc operates its UK operates through Power Leisure Bookmakers Limited ("PLB") which maintains a separate privacy policy. PLB is registered as a Data Controller with the ICO and details are published on a public register on the ICO website at* ***http://ico.org.uk*** *.*

34. Thus, if individuals visit or use a branded SBG platform they may interact with various data controllers but be unable to know which entity is actually processing their data or determining the purposes and means of that processing. For instance, where a data subject visits "*Sky Bet*", the Notice suggests that seven companies could be controllers:

    34.1. Sky Betting and Gaming

    34.2. The Flutter Group

    34.3. Flutter Entertainment Plc

    34.4. Hestview Limited

    34.5. Bonne Terre Limited

    34.6. Core Gaming Limited

    34.7. Power Leisure Bookmakers Limited

35. Individuals that visit an SBG website cannot know which of these seven companies processes their personal data or which entity is the data controller based on the information provided in the Notice. Further, it is unsatisfactory to have seven separate companies listed as potentially involved in data processing activities (especially when only some of those companies are registered with the Information Commissioner).

36. This ambiguity is a significant barrier to data subjects in understanding how their data is being processed, assessing whether such processing is lawful, and exercising their rights in relation to it. This problem is compounded by the failure to provide sufficient transparency over the data processing activities that one or more of the SBG Group of companies are involved in.

37. What is more, this first issue renders it particularly unlikely that a data subject will have the ability and resources to bring litigation in respect of any of the other issues set out below, because so much time and effort will be expended in trying to identify the correct legal entity (or entities) to be the defendant to a claim. Only

the regulator will have the capacity and powers to identify what entities are properly the controllers for what acts of processing.

II. Legal bases for processing

Background

38. For the processing of personal data to be "*lawful*" for the purposes of Article 5(1)(a) UK GDPR, at least one of the conditions under Article 6 UK GDPR must apply. The Notice sets out the purported legal bases for processing. The legal bases cited within the Notice are defective and inconsistent with the UK GDPR.

39. The Notice states that the SBG companies rely on consent for "marketing", in the following terms: "*Things we do with your consent: Marketing*". Such "*marketing*" is said to include "*profiling*". That "*profiling*" includes the detailed behavioural profiling as set out in the Report. Thus, the Notice confirms that SBG rely on consent within Article 6(1)(a) UK GDPR for such processing.

40. The Notice separately lists data processing that SBG conducts for "*personalisation*" purposes. Under "*giving you a more personal experience*", SBG list a range of "*personalisation*" features, including showing users "*the type of score card or bet slip that best suits [their] style of betting*" and "*remind[ing users] to deposit funds when [their] account is running low*". SBG do not nominate any legal basis for this processing in the Notice. Instead, they assert:

> *"We believe this personalised experience makes betting and gaming better and we want to give you the best customer experience we can. Using your personal data in this way enables us to do that in a way that we believe does not have an impact on your privacy. If you don't want your data used in this way your option is to not use our services and to close your account."*

The law

41. The burden of demonstrating that consent has validly been provided by data subjects rests with the controller, under Articles 5(2) and 7(1) UK GDPR. Consent is defined in Article 4(11) UK GDPR as the "*freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a*

statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

42. Recitals (32), (42) and (43) UK GDPR provide some further context to the requirements of consent:

> *(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*
>
> *…*
>
> *(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC ([10]) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given*

if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

43. In addition to these base requirements, Article 7 UK GDPR specifies further conditions for consent. Elements that are germane to SBG include:

    43.1. **Article 7(2)** – Consent should not be buried or bundled within other terms when given as part of a written declaration. Rather, such consent must be "*clearly distinguishable from the other matters*" within that written declaration.

    43.2. **Article 7(3)** – Data subjects must be afforded the right to withdraw consent. The data controller is obliged to make it "*as easy to withdraw as to give consent*."

    43.3. **Article 7(4)** – The default position in a contract should be given weight when considering whether consent is "*freely given*".

44. The European Data Protection Board Guidelines on Consent[7] ("**EDPB Guidance"** herein) provide a helpful overview of what these requirements mean in practice:

[7] Guidelines 05/2020 on consent under Regulation 2016/679 (4 May 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

i. **Freely given** – This means there must be "*real choice and control for data subjects*"[8]. Such free choice may be impacted where there is an imbalance of power between the data controller and the data subject. Real choice would also be undermined if consent is made conditional or that consent is not sufficiently granular (i.e. the data controller does not conflate purposes for processing).

i. **Specific** – The Guidance on Consent confirms that "*The requirement that consent must be 'specific' aims to ensure a degree of user control and transparency for the data subject.*" In turn, the Guidance on Consent suggests that "*to comply with the element of 'specific'*" the data controller "*must apply: (i) Purpose specification as a safeguard against function creep, (ii) Granularity in consent requests; and (iii) Clear separation of information related to obtaining consent for data processing activities from information about other matters*"[9].

ii. **Informed** – The Guidance on Consent provides "*Minimum content requirements for consent to be 'informed'*"[10]. This is information that must be provided to ensure that a data subject is sufficiently "*informed*" for consent to be validly given. The guidelines also state that where "…*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*."

iii. **Unambiguous indication of the data subject's wishes** – This is where an individual, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject must have taken a deliberate action to consent to the particular processing.

45. The Guidance on Consent highlights that:

> *"Explicit consent is required in certain situations where serious data protection risk emerge, hence, where a high level of individual control over personal data is deemed appropriate. Under the GDPR, explicit consent*

[8] At para 13
[9] At para 55
[10] At para 64

plays a role in Article 9 on the processing of special categories of data, the provisions on data transfers to third countries or international organisations in the absence of adequate safeguards in Article 49, and in Article 22 on automated individual decision-making, including profiling."[11]

46. The Court of Justice of the European Union ("**CJEU**") have also considered requirements for consent, finding that consent must be "'*specific' in the sense that it must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes*"[12]. The CJEU has further found that "*a user must be in a position to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed. It must be clearly comprehensible and sufficiently detailed so as to enable the user to comprehend the functioning of the cookies employed*"[13]. The CJEU have found that for consent to be valid, it requires a controller such as SBG to:

> *… provide the data subject with information relating to all the circumstances surrounding the data processing, in an intelligible and easily accessible form, using clear and plain language, allowing the data subject to be aware of, inter alia, the type of data to be processed, the identity of the controller, the period and procedures for that processing and the purposes of the processing. Such information must enable the data subject to be able to determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed.*[14]

47. These cases have been described by the Upper Tribunal (Administrative Appeals Chamber) as follows:

---

[11] At para 91
[12] *Case C-673/17 Verbraucherzentrale Bundesverband eV v Planet49 GmbH* [2020] 1 WLR 2248 (EU:C:2019:801) at para 58. While *Planet49* related to cookies and the e-Privacy Directive, this part of its reasoning has been expressly adopted and repeated by the CJEU in subsequent cases concerned with the data protection regime: e.g. Case C-61/19 *Orange Romania SA v ANSPDCP* (EU:C:2020:901) at para 40.
[13] Ibid at para 74
[14] Case C-61/19 *Orange Romania SA v ANSPDCP* (EU:C:2020:901) at para 40. See too Case C-102/20 *StWL Städtische Werke Lauf a.d. Pegnitz GmbH v eprimo GmbH* (EU:C:2021:954) at para 59

> *The decisions are especially helpful as regard the requirement that consent be both "specific" and "informed". They* ***set a relatively high bar to be met for a valid consent****.*[15] (emphasis added)

48. The ICO's own guidance on consent confirms that SBG must "*provide granular consent options for each separate type of processing*". The ICO approach is consistent with the EDPB Guidance, which requires a controller to provide "*specific information… about the data that are processed for each purpose*".

49. Clean Up Gambling apply specific features of the case law and guidance on consent to SBG's reliance on consent below.

Application to facts

50. SBG's reliance on consent is misplaced and contrary to the UK GDPR. The consent relied on is invalid and SBG do not have a lawful basis for their processing. (No other basis has been identified by SBG, and nor could it sensibly be given the nature of the processing.)

51. **Profiling** – The Report demonstrates that SBG engage in extensive profiling based on individual behaviours and gambling predilections. The Notice confirms that SBG engages in behavioural profiling, asserting that:

> *we look at what we know about you – such as your age, location and gender, your browsing, betting and gaming history and patterns, your social media usage and how you interact with us – and we use it to build up a picture of you that helps us decide what you're most likely to want to hear about. (This is sometimes known as 'Profiling').*

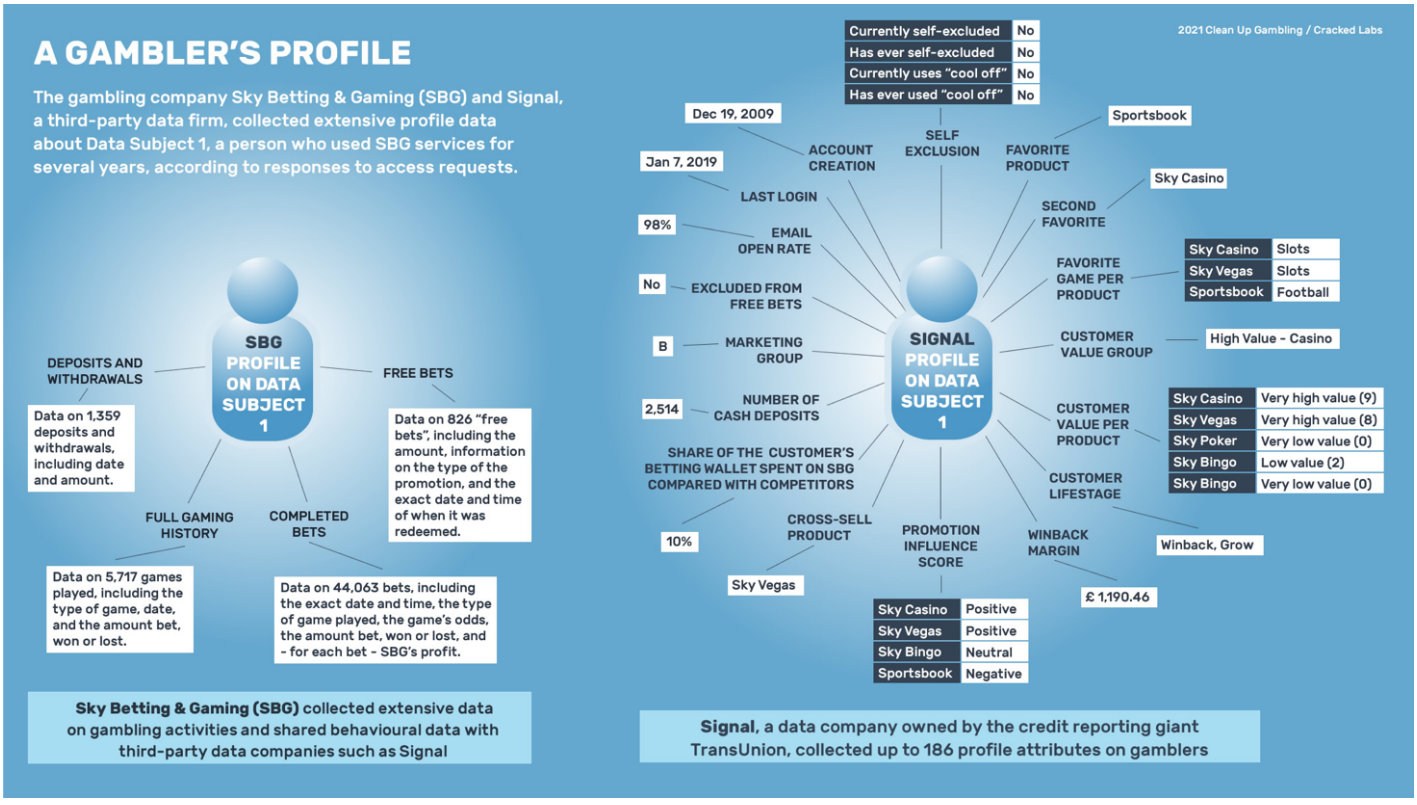
52. The Report sets out how this profiling occurs. In particular, the Report ascertains that SBG engages a network of third-party companies to conduct such profiling. For instance, SBG engaged a US based company, Signal Inc, to profile individuals based on their behaviour. The Report shows that Signal retained detailed personal profiles revealing intimate gambling behaviour. The Report shows a Signal file which contained 186 separate attributes for a single

---

[15] *Leave.EU Group Ltd v Information Commissioner* [2021] UKUT 26 (AAC) at para 51

individual. Those 186 attributes painted a detailed and personal portrait of the individual's gambling behaviour, including their propensity to gamble, their favourite games, and their susceptibility to marketing. The profiles also included metrics as to how much they are worth financially to the gambling companies and categorised individuals on their inferred "value" to operators. SBG use this profiling to make decisions that significantly impact their customers' use of their websites, for example whether and when to offer 'free spins' in order to tempt individuals back into gambling at the most opportune (i.e., vulnerable) moment. This is an extraordinarily harmful form of processing, which is materially different from much of the profiling and data broking activity which otherwise attracts concern: it does not simply result in marketing which may encourage a consumer to purchase a product they would not otherwise have purchased, but rather encourages those vulnerable to gambling addiction to keep gambling, and to lose life-changing amounts of money in very short periods of time.

53. The Report provides an illustration of the profiling data processed by SBG and Signal:



54. SBG's reliance on consent for such practices is flawed. SBG do not provide data subjects with any details of the processing that leads to the profile in this illustration within the Notice or anywhere else. This lack of information means that the consent SBG seeks to obtain is not informed and cannot meet UK GDPR thresholds. It does not come close to meeting the legal standards set in the CJEU's case law.

55. Further, SBG do not explain what data is involved in their processing, nor the output profile data that results from the processing. Rather, the Notice refers to SBG using data to "*build up a picture of you that helps us decide what you're most likely to want to hear about*". This wording does not provide sufficient specificity as to the extent of processing, as it does not address what processing is involved in SBG "*building up a picture*" of a data subject. The Notice also does not explain what the outcome of that processing will be or the likely consequences for data subjects. For instance, the Notice does not explain that the profiling includes detailed analysis of whether an individual is influenced by marketing. Given the potential harms to data subjects, this lack of information is of real significance.

56. The Report sets out how the use of SBG's websites results in the transmission of personal data to dozens different third-party companies, some of whom go on further transmit that data to yet more companies. The sheer scale of this network would be impossible to meaningfully explain to an individual user, who would need to read the privacy notices of many (tens of) different companies. The nature of the processing is not consistent with the use of consent as a legal basis. The purported consent is, in reality, designed to be a blank cheque.

57. In practice, a data subject cannot "*determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed*." Individuals simply do not know what is happening with their data, so cannot be said to have consented to the use of their data in that way. Rather, individuals presented with the detailed portrait of their behaviour have expressed shock at

the level of detail.[16] That shock provides powerful supporting evidence that those individuals had not validly consented to such profiling. As such, the Notice does not provide sufficient specificity to meet the thresholds on consent.

58. **Third parties** – Recital (42) requires SBG to identify the controllers that would process data. The ICO guidance on consent confirms that this requires SBG to "*name any third-party controllers who will be relying on the consent*." The Notice makes no mention of any third party for profiling, such as Signal. Moreover, SBG do not refer to the use of Signal for profiling in response to access requests.

59. The Report moreover demonstrates that SBG engage a plethora of third-party profiling companies, finding that "*even limited browsing of 37 visits to gambling websites led to 2,154 data transmissions to 83 domains controlled by 44 different companies.*" Those companies include Facebook, Google, MediaMath, Adobe and other data brokers. SBG do not name these companies on the Notice, nor elsewhere provide data subjects with information about these third-parties. Those companies were not named in response to access requests.

60. The Report also demonstrates that a visit to a SBG platform triggers onward processing by third parties to several other controllers (as to which, see para 80 below).

61. None of this processing is explained to a data subject. Data subjects cannot be providing "*specific*" and "*informed*" consent if they are not informed about the specific companies involved in profiling them. Conversely, individuals cannot refuse to consent to such practices (or later withdraw their consent) if they are not informed of them.

62. This lack of information is inconsistent with the need to provide data subjects with information to allow them to "*determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed*."

---

[16] See, BBC Panorama, *Paul Merson: Football, Gambling and Me* (https://www.bbc.co.uk/programmes/m0010l43) at 37m – 41m. See also references at footnote 4

63. **Withdrawing consent** – The Notice presents a confusing double layer of options to individuals, as follows

> *… our direct marketing is tailored to you in this way, so to opt out of this type of personalisation you will need to opt out of receiving all direct marketing from us. You can do this when you sign up, by not ticking the box to opt in to marketing, or at any later point via your online account, and SkyBet customers in Germany can also do this via their online preference centre. We won't then send you offers and information by post, email or SMS <u>but we will continue to personalise your online experience onsite and across social media based on the picture we've built up of you</u>.* (Emphasis added)

64. Thus, even if a data subject opts-out from marketing, the Notice confirms they will continue to be subject to extensive behavioural profiling for the purposes of *inter alia*, "*Targeted messages on social media platforms such as Facebook or Twitter (which you can control easily through your privacy settings on each individual platform) and in other places on the internet that support targeted advertising.*" This constitutes a failure to give effect to a data subject's rights and/or to discourage their use by asserting that they will be ineffective.

65. The Notice further states that "*if you prefer not to receive any personalised messages or offers online you can opt out by clicking here, or through your online account.*" However, the reference to "*clicking here*" is simply text without any hyperlink or operative function. There are no settings within the online account that allow for removal of such profiling. Even if data subjects could opt out through a hyperlink, the Notice states that SBG would still "*personalise*" users which includes "*[s]ome personalised banner <u>adverts</u>*" through the deployment of cookies (see further in paras 80 to 101).

66. In practice, therefore, individuals do not have agency or choice over such processing and the consent purportedly collected is not valid.

67. **Consent by default and bundling of consent** – SBG turn on personalisation by default. Even if an individual opts out from marketing, this does not turn off profiling and processing related to personalisation (which includes marketing).

Rather, a data subject is required to search for an unspecified link within their "*online account*" and in practice, an option to turn off personalisation does not exist. Such an approach is inconsistent with the conditions on consent as (i) it is not "*as easy*" to withdraw consent as it was for a data subject to provide it, contrary to Article 7(3) UK GDPR (indeed, it is not possible at all); and (ii) consent is defaulted on as part of a user's agreement to the contract, contrary to Article 7(4) UK GDPR. The UK GDPR requires clear affirmative action to receive consent, as clarified in Recital (32).

68. As the ICO Guidance further clarifies:

> *It must be obvious that the individual has consented, and what they have consented to. This requires more than just a confirmation that they have read terms and conditions – there must be a clear signal that they agree. If there is any room for doubt, it is not valid consent.*
>
> *[…]*
>
> *The key point is that all consent must be opt-in consent, ie a positive action or indication – there is no such thing as 'opt-out consent'. Failure to opt out is not consent as it does not involve a clear affirmative act. You may not rely on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions, or seek to take advantage of inertia, inattention or default bias in any other way. All of these methods also involve ambiguity – and for consent to be valid it must be both unambiguous and affirmative. It must be clear that the individual deliberately and actively chose to consent.*

69. The approach by SBG is the antithesis of this approach, relying on opt-out and default settings that are difficult (and perhaps practically impossible) to switch off. Such a default process which requires many steps and different locations to turn off is inconsistent with the requirement to receive an "*freely given*" and "*unambiguous indication*" of the data subject's wishes. Such processing by default is not consistent with the requirements for consent. Indeed, it appears that SBG do not offer a service without "*personalised*" content and profiling, which is inconsistent with Article 7(4) UK GDPR.

70. **Summary:** SBG's reliance on consent is non-compliant with the requirements of the UK GDPR as such consent is not based on "*specific*" information such that data subjects can provide "*informed*" consent. Moreover, data subjects are opted into such processing by default, contrary to the requirements on providing an "*unambiguous indication*" of individual choices. The result is that data subjects cannot "*determine easily the consequences of any consent he or she might give and ensure that the consent given is well informed*." Data subjects are also prevented from withdrawing their purported consent to the processing. SBG's attempts to rely on consent for a broad range of processing for the purposes of profiling, marketing and personalisation are incompatible with the standards imposed by the UK GDPR and are invalid.

71. **Action the ICO is requested to take**: SBG's reliance on consent is not consistent with the requirements of the UK GDPR. Nevertheless, the processing reliant on that consent has resulted in systemic profiling and widespread dissemination of personal data to third parties. The Report highlights extensive profiling by SBG and third parties who rely on the purported consent obtained by SBG. Indeed, at least the 44 different companies identified in the Report rely on SBG's invalid consent and then transfer that data onwards to many more companies.

72. The Report demonstrates that every interaction by anonymous visitors and registered users with the various SBG platforms lead to detailed and extensive behavioural profiling, none of which has a valid legal basis. It is imperative that the Commissioner take steps to audit SBG, and take subsequent enforcement action, to ensure:

    72.1. That all data controllers processing the personal data of visitors and users of SBG's platforms have a valid legal basis for that processing, including providing individuals with real choice; and

    72.2. All data collected and profiles developed in reliance on invalid consent are deleted.

73. The Commissioner is uniquely placed to protect individuals, in a way that each individual impacted by this widespread unlawful processing cannot do for themselves. The Commissioner should act to rectify this unlawful processing and the harmful profiling that it has enabled.

III. Special category data

74. Special category data is protected by Article 9(1) UK GDPR:

> *"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*

75. A data controller can only process such data if one of the exemptions in Article 9(2) UK GDPR applies.

76. The ICO guidance[17] on the processing of such special category data explains why such data deserves extra protections:

> *"It's not just that this type of information might be seen as more sensitive or 'private'. The recitals to the UK GDPR explain that these types of personal data merit specific protection. This is because use of this data could create significant risks to the individual's fundamental rights and freedoms.*
>
> *[…]*
>
> *The presumption is that this type of data needs to be treated with greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination."*

77. As detailed in Recital (51) UK GDPR,

[17] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

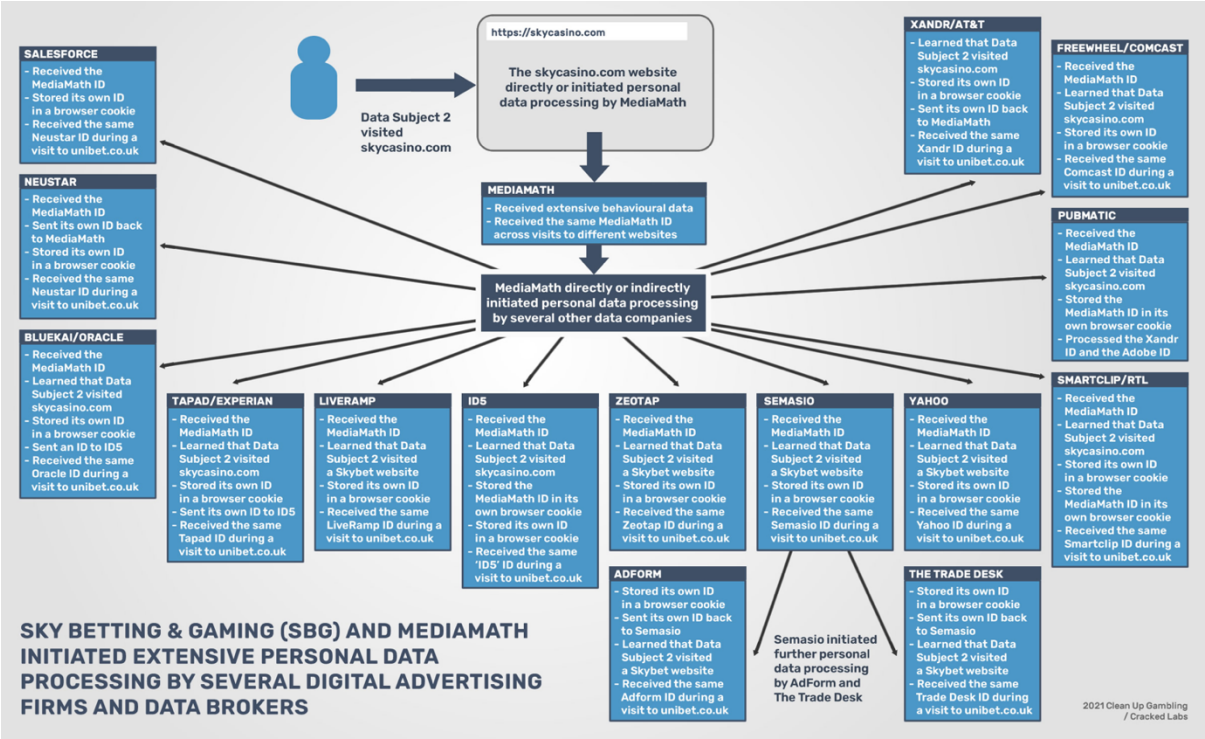
"Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to fundamental rights and freedoms."

78. SBG assert that they do process special category data about an individual's "*physical, psychological or emotional health or situation*". It is unclear precisely what form this data takes, how SBG use this data or for what purposes. It is also unclear whether SBG silo this data so that it is not used for other purposes or what the lawful basis or Article 9 UK GDPR exemption SBG rely on for this processing.

79. Clean Up Gambling are particularly concerned that SBG processes such data without expressly referring to (i) limits to how such data will be used and (ii) the bases under Article 9(2) for such processing. Thus, SBG's processing of data that may reveal individual gambling disorders requires heightened scrutiny, given the "*serious risks*" to individuals from the processing of such data. Accordingly, the ICO should determine whether SBG are processing special category data. If so, the ICO must urgently scrutinise (i) whether SBG limit the processing of such data to specific purposes and (ii) the legal basis for the processing of any special category data. Short of explicit consent, it is extremely difficult to envisage any applicable exemption under Article 9 for such processing.

IV. Use of cookies

80. The Report shows that the profiling conducted by SBG through third-party companies occurs through the deployment of 'cookies'. The Report also demonstrates that SBG facilitate the deployment of cookies for a multitude of other third-party companies, whose relationship with SBG is unclear. Those third-party companies then transfer the personal data of SBG's website visitors onwards to yet other third-party companies, resulting in a vast broadcast of individuals' personal data. The Report illustrates this practice with the following diagram:



81. PECR governs the use of such technology. Regulation 6 of PECR governs the way such technology can be deployed. Regulation 6 extends to cookies and other "*similar technologies*", thus covering techniques such as device fingerprinting deployed by Sky Betting and Gaming and their third-party profiling companies.

82. For such technology to be used, regulation 6(2) requires a user:

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) is given the opportunity to refuse the storage of or access to that information

83. SBG fail to meet both criteria, rendering their deployment of cookies unlawful.

(a) Clear and comprehensive information

84. The ICO has provided guidance on the information to be provided. This includes providing users with information concerning:

84.1. the cookies you intend to use;

84.2. the purposes for which you intend to use them;

84.3. any third parties who may also process information stored in or accessed from the user's device; and

84.4. the duration of any cookies you wish to set.

85. The ICO confirm that this requirement extends to

cookies set by any third parties whose technologies your online service incorporates – this would include cookies, pixels and web beacons, JavaScript and any other means of storing or accessing information on the device including those from other services such as online advertising networks or social media platforms.

86. Thus, users must be notified of (i) the cookies used by SBG and (ii) those set by third parties on SBG platforms. However, SBG does not provide users with this information.

(b) Opportunity to refuse

87. The need for "*the opportunity to refuse the storage of or access to that information*" has been interpreted as a requirement for meaningful consent. PECR itself does not define consent but rather refers to the UK GDPR definition of consent:

"'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

88. The requirements to meet this definition of consent in the UK GDPR is detailed at paras 41 to 48 above. The core issue for users is that they should have real agency over whether cookies are deployed.

89. The CJEU has considered the deployment of cookies and similar technology in several cases. The CJEU has consistently held[18] that the requirement for consent required active, rather than passive, behaviour which was unambiguous. As such, consent given in the form of a preselected tick in a checkbox for cookies did not constitute active behaviour on the part of the website user and did not enable it to be objectively ascertained that the user had actually given their consent. As a result, the fact that a user had not unticked a checkbox that had been pre-ticked by the website provider was not sufficient to constitute "*consent*" for the purposes of those provisions.

90. The ICO summarises[19] these requirements as collectively obliging SBG to take the following steps:

90.1. the user must take a clear and positive action to give their consent to non-essential cookies – continuing to use your website does not constitute valid consent;

90.2. you must clearly inform users about what your cookies are and what they do before they consent to them being set;

90.3. if you use any third party cookies, you must clearly and specifically name who the third parties are and explain what they will do with the information;

---

[18] See, *inter alia*, *Planet 49*

[19] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/

90.4. you cannot use any pre-ticked boxes (or equivalents such as 'on' sliders) for non-essential cookies;

90.5. you must provide users with controls over any non-essential cookies, and still allow users access to your website if they don't consent to these cookies; and

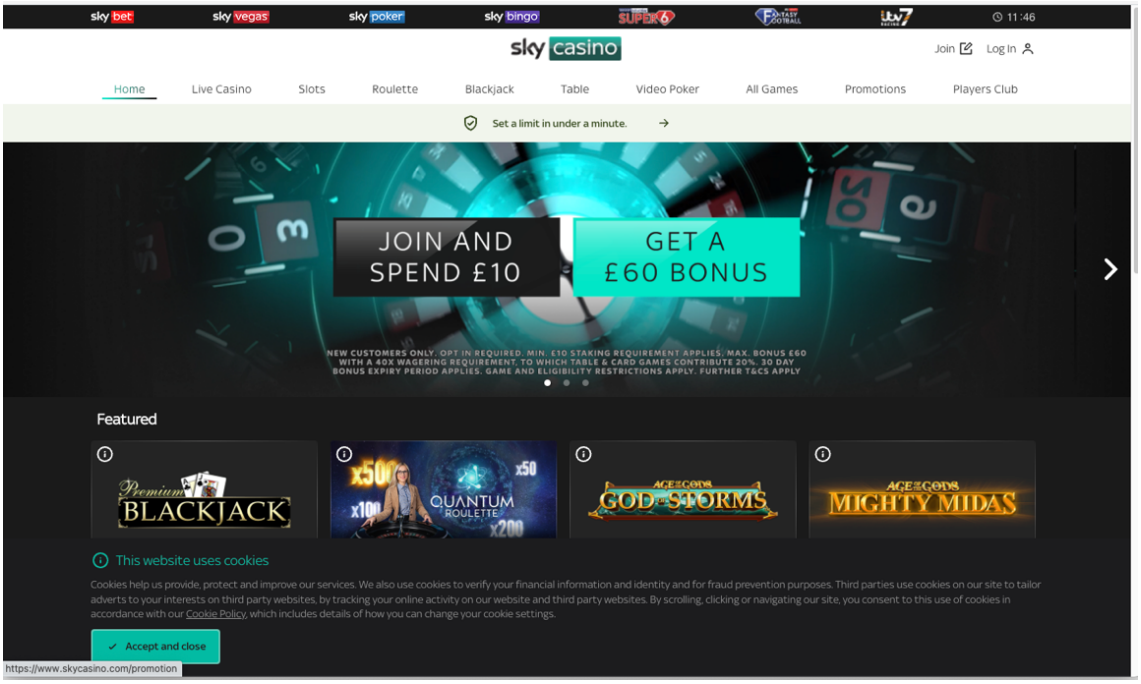
90.6. you must ensure that any non-essential cookies are not placed on your landing page (and similarly that any non-essential scripts or other technologies do not run until the user has given their consent).

91. In practice, SBG do not take these steps. Rather, SBG's approach to the deployment of cookies is flawed, with significant consequences for users.

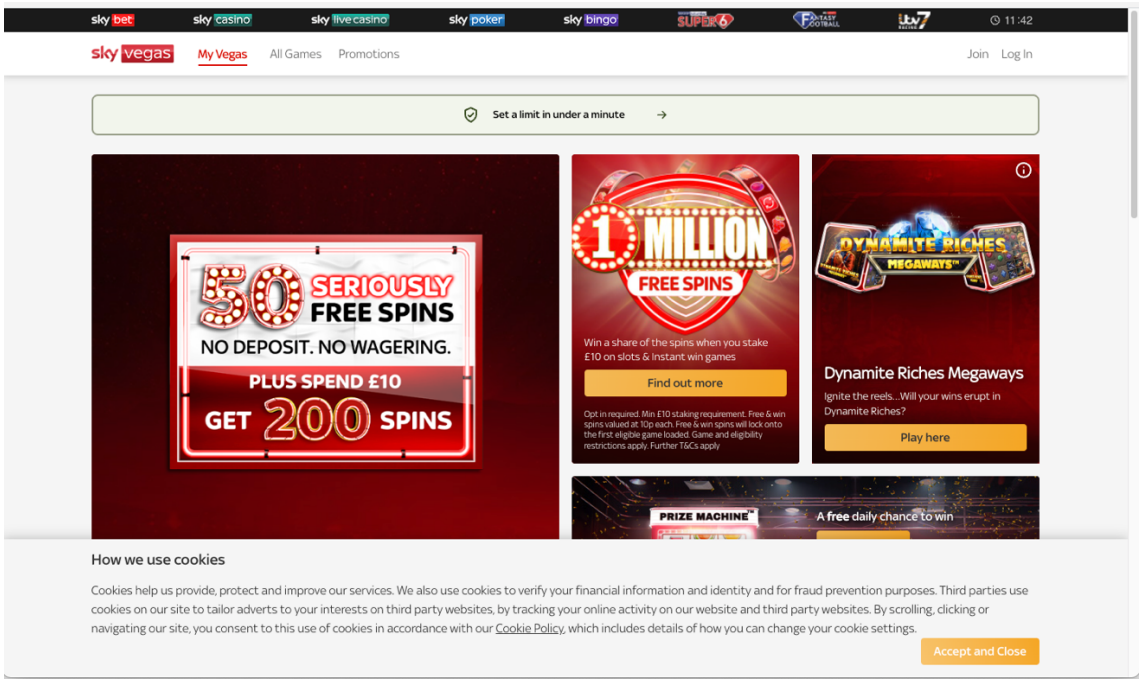
Sky Betting and Gaming's approach to cookies

92. Sky Betting and Gaming's platforms present a single pop-up to visitors first engaging with the websites. Examples of those pop-ups are below:

Sky Casino



Sky Vegas



93. Both these examples are replicated across the SBG suite of platforms. The operative text reads:

> *Cookies help us provide, protect and improve our services. We also use cookies to verify your financial information and identity for fraud prevention purposes. Third parties use cookies on our site to tailor adverts to your interests on third party websites, by tracking your online activity on our website and third party websites. By scrolling, clicking or navigating our site, you consent to the use of cookies in accordance with our Cookie Policy, which includes details of how you can change your cookie settings.*
>
> ***Accept and Close***

94. The Cookie Policy is available as part of the Notice, which states:

> *All modern browsers allow you to see what cookies you have, and to clear them individually or in their entirety by changing your cookie settings. Cookie settings are typically found in the 'options' or 'preferences' menu of your browser, otherwise you should use the 'Help' option in your browser for more details.*

95. Thus, individuals are not provided with granular information about the cookies that will be deployed. Individuals are also not given any option to refuse the deployment of cookies, either at the time they are deployed or otherwise.

Application of law to facts

96. The SBG platform's use of cookies is not consistent with the requirements of PECR:

96.1. **No specificity** – Users are not provided with sufficient specificity about the cookies that will be deployed. Rather, users are told in vague and generic terms that technology will be deployed for certain SBG services. Users are not told that such technology will be used to build detailed behavioural profiles. Moreover, users are not told that such profiles will be compiled with and by third parties, nor are those third parties named.

96.2. **No option to refuse** – Users are not given an option to refuse the deployment of cookies and similar technology, contrary to regulation 6(2)(b) PECR. Rather, users are only given an option to "*accept and close*" the deployment of cookies. In effect, SBG deploy a default opt-in to cookies, such that a user is not invited to make a "*clear and positive*" action to give their consent. Such an "*all or nothing*" approach can be contrasted to, for example, the consent considered by the CJEU in *Planet49*. In that case, Planet49 defaulted to an opt-in check box but still allowed users to uncheck a box. Thus, there was a level of control. Nevertheless, the CJEU found such a pre-ticked box to be inconsistent with the requirements on consent for the purposes of regulation 6. SBG offer no option at all to users. SBG do not therefore receive "*consent*" for the deployment of such cookies.

97. SBG further claim that "*scrolling, clicking or navigating*" their platforms amounts to consent. Such an approach is inconsistent with the definition of consent requiring active choice by a user and that "*silence or inactivity does not constitute*

consent."[20] If correct, it would in practice denude regulation 6 of any real practical relevance. As the ICO confirm "*continuing to use your website does not constitute valid consent*".[21]

98. The Notice is of no assistance to SBG. The Notice refers to cookie settings on a user's browser, rather than, as regulation 6(2)(b) requires, providing an option to refuse the deployment of specific technology. The Notice is hopelessly inconsistent with the PECR requirements.

99. Taken together, SBG do not receive consent from visitors or users for the deployment of cookies. As a consequence, the plethora of third-party companies that deploy cookies on the Sky Betting and Gaming platforms, such as Signal, MediaMath, Adobe, Facebook, and Google also lack the consent they require to deploy cookies lawfully.

100. Pursuant to regulation 32 PECR, Clean Up Gambling requests the Commissioner to take enforcement action, including the following steps:

    100.1. Confirm whether SBG receive valid consent for the deployment of cookies or not.

    100.2. Take action to audit which third parties companies are deploying cookies and similar technology on SBG platforms in reliance on this purported consent

    100.3. Mandate SBG to erase information collected as a result of the unlawful deployment of cookies.

    100.4. Take steps, as far as possible, to ensure that data collected by third parties as identified in the Report is erased as a result of the unlawful deployment of cookies.

---

[20] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/#:~:text=Silence%2C%20pre%2Dticked%20boxes%20or,as%20an%20opt%2Din%20box.

[21] https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/

101. This request is made to the Commissioner given the Commissioner's statutory role to uphold PECR. The longstanding contravention of PECR has caused real-world harms, in the form of extensive and covert behavioural profiling identified in the Report. The Commissioner is uniquely empowered to ameliorate those harms.

V. Transparency

102. The Report details the extensive data processing both within the SBG group and by third parties facilitated by SBG. The Notice does not however allow an individual to know how their data has been or will be processed, or the consequences of that processing. The Notice does not meet the requirements for transparent processing, contrary to Article 5(1)(a) UK GDPR, and Articles 12 – 14 UK GDPR on the modalities of transparency.

103. The Information Commissioner has provided useful guidance on transparency[22]:

103.1. The Commissioner states that transparency is "*fundamentally linked to fairness*", which is about being "*clear, open and honest with people from the start about who you are, and how and why you use their personal data.*"

103.2. Transparency is of heightened importance "*in situations where individuals have a choice about whether they wish to enter into a relationship with you*". If individuals know at the outset what you will use their information for, they will be able to make an informed decision about whether to enter into a relationship, or perhaps to try to renegotiate the terms of that relationship.

103.3. The Commissioner confirms that transparency is (emphasis added) "*important even when you have no direct relationship with the individual and collect their personal data from another source. In some cases, it can be even more important – as individuals may have no idea that you are*

[22] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

collecting and using their personal data, and this affects their ability to assert their rights over their data. This is sometimes known as 'invisible processing'." This guidance is particularly important when considering the role of third parties, such as those deployed and facilitated by SBG, to conduct profiling of data subjects.

103.4. What transparency requires will be context-specific. Important factors in that context include the risk of harm to the data subject from the processing, the sensitivity of the personal data, the intrusiveness of the processing and the degree to which the data is to be used by others as part of a wider ecosystem. The context of SBG's processing is a particular serious and significant one. The more serious and significant the processing, the greater the imperative that it be explained at the outset, in clear and plain terms which do not unduly 'spin' the debate. The Commissioner is invited to contrast the context here with that set out in the Enforcement Notice issued to Experian, where high standards of transparency were rightly required in a processing context not nearly so significant as the present (albeit on a much larger scale).

104. In the Commissioner's report on direct marketing,[23] the Commissioner highlighted that the need for transparency is greater where the controller has no active relationship with a data subject, as:

> *"If privacy information is not actively provided then this can cause 'invisible' processing – it is 'invisible' because the individual is not aware that the organisation is collecting and using their personal data."*

105. Despite the obligations for transparency set out in the UK GDPR, the Notice falls well short of what is required for SBG to meet these obligations.

Application to facts

[23] https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf

106. The Notice does not provide sufficient information for a data subject to know what data may be collected about them or how their data may be used by SBG:

106.1. Contrary to Articles 13(1)(a) and 14(1)(a) UK GDPR, the Notice does not identify the controller, as it refers to an entity (namely, SBG) that does not have legal personality. Moreover, the Notice refers to internal sharing of data within the group of companies, but does not provide a complete list of the group of companies, describe nor define the respective data processing activities and role (controller, joint controller, processor) of each company.

106.2. Contrary to Articles 13(1)(c) and 14(1)(c) UK GDPR, the Notice does not provide sufficient specificity of the purposes of the data processing. To the extent that information on purposes is provided, vague language is used, such as "*decide what you're most likely to want to hear about*" which obscures the fact that much of SBG's processing aims at maximising customers' time on their platforms. The impact of such engagement is problematic in a gambling context, where the result is losses of money. The failure to comply with the purpose limitation principle is set out further below.

106.3. Contrary to Articles 13(1)(e) and 14(1)(e) UK GDPR, the Notice does not specify the recipients or categories of recipients of personal data. Rather, the Notice refers in generic terms to data sharing with unspecified third parties. This is particularly pronounced where SBG may have shared special category data relating to individual data subject's addiction to online gaming (or vulnerability to such an addiction).

107. Under Article 5(2) UK GDPR, SBG have the burden of showing compliance with the data protection principles. As set out above, SBG are not processing data transparently and are thus in breach of Article 5(1)(a) UK GDPR.

108. It is entirely apt to describe the processing of SBG as 'invisible'. As the Commissioner explained in the Experian Enforcement Notice, the onus should not be on individuals to trawl through the privacy policies of these companies or

to make access requests to receive information about how their data is being processed. That would be to fundamentally reverse the nature of the obligations imposed on controllers.

109. The Article 29 Working Party stated that the more intrusive (or less expected) the processing is, the more important it is to provide information to individuals in advance of the processing (in accordance with Articles 13 and 14 GDPR).[24] The processing of SBG's website visitors' data is both unexpected and highly intrusive:

    109.1. SBG's website visitors may expect that SBG itself processes their data about the use of SBG sites to make their sites and games function. They are very unlikely to expect SBG to combine this with other personal data – including that sourced from data brokers – to build up individual behavioural profiles on them. Much less are they likely to expect that SBG would work with dozens of third-party companies to facilitate this processing and profiling, or that because of having a cookie stored in their browser on visiting an SBG site, they will then be tracked when they visit websites of completely unconnected companies.

    109.2. Online gambling has the propensity to cause serious harm to individuals. Profiling individuals on their addictive behaviours, their susceptibility to gamble and what games they are addicted to (or can be led to become addicted to), as well as how they are influenced by marketing may increase the risk of both financial and psychological harm, making it highly intrusive.

110. The nature of SBG's processing and its potential consequences ought to imply a very high standard of transparency for visitors to its websites. This makes their failure to meet even basic transparency requirements about their processing particularly concerning.

VI. <u>Retention periods</u>

[24] Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)

The law

111. Article 5(1)(e) UK GDPR requires personal data to be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).*"

112. Recital (39) UK GDPR further confirms

> *The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.*

113. The ICO Guidance on storage limitation confirms that this principle means that "*even if you collect and use personal data fairly and lawfully, you cannot keep it for longer than you actually need it.*"[25] The ICO guidance further confirms that the burden is on the controller to justify the periods: "*You must also be able to justify why you need to keep personal data in a form that permits identification of individuals.*"[26] This position is consistent with Article 5(2) UK GDPR.

Application to facts

114. The Notice does not specify the retention periods applicable. Rather, SBG states that:

> *"[we] hold your personal information only as long as we have a valid legal reason to do so, which includes providing you with the services you have*

---

[25] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/#:~:text=What%20is%20the%20storage%20limitation%20principle%3F,-Article%205(1&text=So%2C%20even%20if%20you%20collect,for%20different%20types%20of%20data.

[26] *Ibid*

requested, meeting our legal and regulatory obligations, resolving disputes and enforcing our agreements."

115. A data subject cannot therefore know the retention periods for their data, contrary to Articles 13(2)(a), or at a minimum the criteria used to determine the periods, contrary to 14(2)(a) UK GDPR. This failure to have clear and precise retention policies means SBG cannot also demonstrate compliance with Articles 5(1)(c) and 5(1)(e) UK GDPR.

116. The Report highlights that, in practice, SBG retained an individual's entire history of interactions with their platforms for over ten years. That included every bet placed, every advert sent and every other interaction with SBG. Such retention is not consistent with Article 5(1)(e) UK GDPR, as this cannot be "necessary". Thus, SBG's retention policies – so far as they can be said to exist at all – do not comply with the UK GDPR.

VII. Rights of data subjects

117. The Report highlights difficulties that data subjects have had in attempting to assert their rights afforded by the UK GDPR. Those problems are aggravated by the Notice. Taken together, individuals face difficulties in asserting the rights under the UK GDPR. For example:

117.1. The Report details the difficulties in understanding the complex web of third-party actors involved in processing data following visits to websites. Individuals are not informed about these third parties in response to subject access requests under the UK GDPR. Ordinary users are also unable to carry out the expert browser observation undertaken for the Report and would therefore have no way of knowing that the access request responses are deficient and challenging them. Thus, even where individuals take the step of making a subject access request they cannot exercise any control over how SBG and third parties process their personal data. That problem is aggravated by a lack of information on the Notice about those third parties.

117.2. Specific timeframes for retention of data are not provided to data subjects within the Notice. Rather, a data subject is forced to rely on the discretion of SBG. In practice, SBG retain data indefinitely.

117.3. Article 21(2) UK GDPR provides an individual with an unqualified "right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing." Thus, individuals should be presented with an unqualified and complete right to object to processing for direct marketing, including profiling. Article 21(4) provides that "At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information." SBG however only provide a very limited right to object. The Notice states that (emphasis added):

> *Data protection law gives you the right to express an objection to activities detailed in the section entitled* ***'Running our business effectively and efficiently'*** *if you believe your privacy rights outweigh the legitimate interest we have as a business in doing those things. Please read that section carefully before getting in touch with us and note that exercising your right of objection will usually mean you need to close your account and stop using our services. If you disagree with our decision on this, you have the right to complain to the* ***privacy regulator.***

Thus, an individual cannot exercise the right to object to processing for direct marketing. Rather, they are told that they will have their account closed for exercising their right. This is an obvious and egregious frustration of the rights of the data subject, penalising them for exercising a right afforded by law.

118. These are examples of the problems that data subjects face. Those problems are aggravated by the lack of transparency about (i) who the controllers are and (ii) what data is being processed.

119. In the same way that the Commissioner has sought greater control for data subjects over data held by credit reference agencies and data broking companies, Clean Up Gambling requests the Commissioner to take enforcement action against SBG and others within the online gambling industry to ensure that individuals' data rights are respected.

VIII. Purpose limitation

120. The obligations on SBG to identify their "*purposes*" are found, in particular, in the following provisions of the UK GDPR:

120.1. The second data protection principle, as contained in Article 5(1)(b), which requires personal data to be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes… ('purpose limitation')*";

120.2. The provision of information including "*the purposes of the processing for which the personal data are intended as well as the legal bases for processing*", as per Articles 12(1), 13(1)(c) and 14(1)(c); and

120.3. The right to be told "*the purposes of the processing*" under Articles 12(1) and 15(1)(a).

121. Under each of those provisions, SBG is required transparently and explicitly specify the purposes for which the data is collected and processed. SBG have failed to do so. For instance, SBG rely on vague and impossible to decipher phrases such as "*marketing*". It would be unclear to an individual using the services that such marketing includes detailed and extensive behavioural profiling and that such profiling is conducted to anticipate and influence how individuals will act. Moreover, the Notice provides the following rider for how personal data may be used across companies and across (emphasis added):

> *The companies listed within the previous paragraph are wholly owned by Flutter Entertainment Plc. Any reference to "The Flutter Group" within this Privacy Policy includes Flutter Entertainment Plc and all or any of its direct or indirect subsidiary undertakings, joint venture partners, and their related*

companies wherever located in the world as may exist from time to time including, but not limited to, Paddy Power, Betfair, Timeform, Sportsbet, BetEasy, FanDuel, TVG, Adjarabet, Sky Betting and Gaming, Full Tilt, PokerStars and FOX Bet.

[…]

This means that whichever of our products and services you use in any country in which we operate, ***we may share your personal information among all the companies in The Flutter Group for any of the purposes outlined in this policy****.*

122. Thus, any visit to a SBG website may result in any and all personal data being shared amongst the "*Flutter Group*", for "*any of the purposes*" set out in the Notice. This constitutes an explicit statement that SBG does not intend to limit processing of data to specific purposes for which it was collected, nor even limit the data to the data controller with whom a data subject interacts. Rather, a visit to a SBG platform may result in an individuals' behavioural profile being shared with any number of companies within the Flutter group, for any number of purposes. This approach cannot be reconciled with the need in Article 5(1)(b) UK GDPR for data to be collected only for specific and limited purposes.

123. Specification is tied to foreseeability. The ICO guidance on purpose limitation requires a controller to "*be clear from the outset why you are collecting personal data and what you intend to do with it*."[27] Thus, a data controller should be clear and open about their reasons for obtaining personal data before collection and ensure that what they do with the data is in line with the reasonable expectations of the data subject concerned. In turn, a data subject will have an expectation of how their data will be used and must be able to predict what will occur with their data.

[27] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/#:~:text=In%20practice%2C%20this%20means%20that,individuals%20about%20your%20purposes%3B%20and

124. SBG however engage in extensive behavioural profiling. The data that is collected to conduct such behavioural profiling is not explained to a data subject in the Notice but is rather explained in unspecific terms, as follows:

> *we look at what we know about you – such as your age, location and gender, your browsing, betting and gaming history and patterns, your social media usage and how you interact with – and we use it to build up a picture of you that helps us decide what you're most likely to want to hear about.*

125. This language in the Notice can be contrasted with the actual profiling – and the decisions taken based on that profiling – explored in the Report. The dichotomy between what a data subject is told and the processing the occurs means a data subject could not anticipate the actual profiling that does occur. Thus, a data subject cannot expect their data will be used to analyse and influence their behaviour in the manner explored in the Report. Moreover, it is unclear to a data subject what data is collected for these purposes or whether, as seems likely, SBG consider they are entitled to use any and all data it is able to collect about an individual (whether on their website or via third parties) to profile them for marketing, as the Notice is set out in non-exhaustive terms.

126. This problem is aggravated where SBG do not silo data collected so that where an individual exercises their right to opt-out of marketing, their data will not be collected for this separate purpose. Rather, all data collected by SBG is used towards this end. For instance, data collected relating to transactional behaviour related to bets placed is then used to profile individuals on their preferences and provided to third parties, which may then be shared amongst the Flutter Group for any other purpose and without limitation.

127. Thus, SBG collects data in a manner inconsistent with Article 5(1)(b) UK GDPR, as they process all data received for profiling of individuals in a manner that the data subjects cannot anticipate.

IX. 'Dark Patterns' and unfair processing

128. The UK GDPR requires that processing be fair (Article 5(1)(a) UK GDPR). The ICO's own guidance states[28]:

> *[…] fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them […] Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair. […]*
>
> *In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If you have obtained and used the information fairly in relation to most of the people it relates to but unfairly in relation to one individual, there will still be a breach of this principle.*

129. The EDPB has stated in relation to fairness[29]:

> *Fairness is an overarching principle which requires that personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data. See Article 6(1)(b) GDPR.*

130. The EDPB goes on to identify elements of fairness, including:

130.1. **Autonomy and interaction**: data subjects should be able to influence how their data is processed and exercise their data rights.

130.2. **Expectations**: processing should be within data subjects' reasonable expectations.

---

[28] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/#:~:text=In%20general%2C%20fairness%20means%20that,also%20about%20whether%20you%20should.

[29] EDPB Guidelines 04/2019: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

130.3. **Truthful**: data subjects should be provided with information about how their data will be processed, and should not be misled.

130.4. **Non-exploitation**: controllers should not exploit the vulnerabilities of data subjects.

130.5. **Ethical**: controllers should understand and take into account the wider consequences of their processing.

'Dark patterns'

131. The EDPB has further elaborated[30] on the ways in which services may be designed using 'dark patterns': design elements "*that lead users into making unintended, unwilling and potentially harmful decisions regarding the processing of their personal data.*"

132. Specific dark patterns identified by the EDPB include:

132.1. **Skipping**: designing interfaces so that users do not think about data protection.

132.2. **Hindering;** preventing users from being informed or making choices about their data through *dead ends* in interfaces and providing *misleading information*.

132.3. **Left in the dark**: where users left unsure of how their data is processed or the extent to which they can influence it due to *ambiguous wording or information.*

Application to facts

133. SBG's processing of personal data meets a number of the EDPB's definitions of unfairness, and the design of its websites and wording of its Notice typify a number of the dark patterns which the EDPB has identified. This strongly

[30] EDPB Guidelines 03/2022: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

indicates that SBG's processing of personal data is fundamentally unfair and therefore unlawful:

133.1. **Autonomy and interaction:** this submission and the Report set out how SBG puts barriers in the way of its users controlling how their data is processed, for example by defaulting consent (para 67), providing marketing 'opt outs' which do not stop all marketing processing (see paras 63 to 64), referring to links to fully opt out that do not exist (para 65), and providing deficient responses to subject access requests (para 117). These design choices also typify the dark patterns of **skipping** and **hindering**.

133.2. **Expectations:** this Submission details how the range of purposes for which SBG processes data (para 121) and the large number of third parties to whom it transmits personal data (and from whom it collects data and inferences, see e.g. paras 56 and 80) cannot possibly be within the reasonable expectations of data subjects.

133.3. **Truthful:** this Submission sets out serious deficiencies in the transparency provided by SBG about its processing (paras 106 to 110) to the point that data subjects cannot know how their data will be processed. This lack of information and ambiguity typifies the dark pattern of **left in the dark**.

133.4. **Non-exploitation and ethical:** The Report and this Submission show how SBG builds intimate profiles of data subjects and makes inferences about their gambling behaviour and how they will respond to marketing. This is done to maximise the amount of time and money that individuals spend online gambling – a behaviour that is apt to form a clinical addiction – and therefore maximise SBG's profits. Its very purpose is to identify and exploit individuals' vulnerability to problem gambling for commercial gain. Considering the extremely serious financial, psychological, and social consequences of problem gambling, the fact that this is a problem growing in scale in the UK, and the fact that this processing is widespread and hidden, it cannot be said that it is ethical.

134. It follows that SBG's processing of personal data is unfair and unlawful.

F. Remedies

135. The Report provides evidence of the extensive, invasive and clandestine profiling conducted by the gambling industry. That profiling focusses on individuals' propensity to gamble, favourite games and susceptibility to marketing, with the ultimate aim of maximising the amount of time and by implication, the money they spend (and therefore lose) on gambling sites.

136. The Report provides extensive information about the scope of the data flows and the web of third-party companies that receive that data to build detailed and intimate profiles of individuals, often without their knowledge. Such profiles include indicators of personal vulnerability and addictive behaviours, which can then be used to target the most vulnerable. Such targeted messaging needs to be seen in the context of the human impact in online gambling.

137. In sum, the gambling industry is able to use the data it collects on individuals to target and exploit the most vulnerable. The data processing that allows for this profiling is however inconsistent with the basic principles of the UK GDPR and PECR. Unlawful processing of personal data with such dire consequences is in urgent need of regulatory action.

138. Taking enforcement action against SBG would fit within the ICO's regulatory action plan ("**RAP**"):

    138.1. **The categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion** – The processing involves special category data, as confirmed by SBG in the Notice. The Report confirms that the behavioural profiles could health data relating to addictive behaviours.

    138.2. **The number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy** – The numbers of individuals is vast and growing rapidly. Online gambling has proliferated, which

increases the risk of vulnerable gamblers being profiled and targeted. Such profiling and targeting leads to financial and psychological harm.

138.3. **The gravity and duration of a breach or potential breach** – The gravity of the breach is exemplified by its scope and scale. SBG do not receive consent for the deployment of tracking technology they use and facilitate. That issue is compounded by the flawed approach to consent for the profiling that follows. The result is widespread and systemic unlawful data practices within SBG. That problem has developed over decades, meaning the controller has processed data unlawfully on a vast number of individuals.

138.4. **Whether the organisation or individual involved is representative of a sector or group, raising the possibility of similar issues arising again across that group or sector if not addressed** – The issues identified in the Report relate to SBG but are indicative of issues that arise across the industry. Indeed, the issues identified in the report are so widespread and systemic across the modern online gambling industry as to be commonplace. Every major online operator engages in some form of behavioural profiling, with equally dubious data protection compliance as SBG. As such, the Commissioner should act to redress practices that grown over decades across an industry

138.5. **The public interest in regulatory action being taken** – There is widespread concern at the behaviour of SBG and its third-party practices. The New York Times ran a long-read piece about the industries approach to profiling. The BBC ran a news story on the main News channel and Clean Up Gambling's work featured in a Panorama special.[31] Such practices were only uncovered because of diligent work by Clean Up Gambling and others rather than proactive transparency from within the industry. That cannot be permitted to continue.

[31] See footnote 4

139. The industry and issues identified in the Report also meet some of the "aggravating" features identified in the RAP:

139.1. **Whether the attitude and conduct of the individual or organisation concerned suggests an intentional, wilful or negligent approach to compliance or unlawful business or operating model** – The Report and these submissions demonstrate that SBG is at best reckless when approaching data protection. For instance, SBG's approach to the deployment of cookies is contrary to the basic requirements of PECR as users are given no choice to refuse such technology. Further, the legal bases for profiling are flawed as individuals are not able to consent to such practices. No other legal basis is provided. Given the scale of the profiling undertaken, SBG's approach to profiling is reckless and, insofar as their business model relies on proofing, that business model must be rectified to ensure individuals are aware of how their data will be used. There must be at least a realistic possibility that an investigation carried out by the Commissioner would conclude that at least aspects of SBG's conduct are designed deliberately in a non-compliant manner.

139.2. **The vulnerability, if any, of the individuals affected** – The individuals affected are potentially very vulnerable. Indeed, SBG confirm in the Notice that they will process special category data relating to the vulnerability of individuals who use their platform. Gambling addiction is a recognised psychological disorder, which the data processing activities identified in the Report may aggravate.

140. In Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd* (EU:C:2020:559) at para 108 the CJEU held that "*the supervisory authorities' primary responsibility is to monitor the application of the GDPR and to ensure its enforcement.*" Authorities such as the Commissioner must, for example, handle complaints with "*all due diligence*": para 109. At para 112, the CJEU emphasised that the margin of appreciation to be afforded to the supervisory authority is limited:

"*Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence.*"

141. Clean Up Gambling recognises that the commencement of an investigation, particularly one which is or may become a sectoral investigation, of this sort is a matter of discretion for the Commissioner, and that there are many calls on his regulatory priorities. However, the widespread and serious nature of the compliance failures of SBG, taken with the unique nature of the risks of harm involved, render this an investigation an appropriate use of regulatory powers and resources. The online gambling sector, and its use of personal data, is the subject of a significant and increasing media profile.

142. There is no practical alternative to the Commissioner carrying out the tasks imposed on him by the UK GDPR in relation to SBG:

    (1) It is wholly impractical to rely on individual data subjects to commence litigation against SBG, or any linked controller. Leaving aside the difficulty of identifying the correct legal entity against which to bring proceedings, it is noted that: (a) the effect (if not the purpose) of SBG's processing being kept 'invisible' is that only a very small percentage of data subjects who will be sufficiently aware of the processing to be able to act, even if they wished to; (b) the issues are extensive, and may be heavily defended by SBG at great costs; (c) data subjects who have been harmed by the processing, and most likely to wish to litigate, will also be those likely to have suffered significant financial losses (to SBG's benefit) as a result of the processing.

    (2) Online gambling operators are, of course, licensed entities under the Gambling Act 2005 and regulated by the Gambling Commission. Nothing in the gambling legislation purports to address the processing of personal data: that is the sole purview of the UK GDPR and the Commissioner. The Gambling Commission's regulatory functions are limited to those it has

licensed, and its primary tool is the commencement of a licence review process under section 116.[32] The Commissioner has in place a Memorandum of Understanding with the Gambling Commission;[33] no part of that Memorandum purports to attribute responsibility for the issues identified in this Submission to the Gambling Commission. Clean Up Gambling strongly encourages any investigation to be conducted with the support and assistance of the Gambling Commission, but it is essential that data protection compliance failures in the gambling industry do not fall between two regulatory stools, with each regulator assuming the other will address the issue.

143. Given the widespread illegality underpinning the processing by SBG, Clean Up Gambling encourages the Commissioner to commence any such investigation through the issue of Assessment Notices pursuant to section 146 DPA of the relevant entities (as the Commissioner considers them to be). The Commissioner should then take steps to stop processing of personal data that has been collected in contravention of the UK GDPR and PECR, through an Enforcement Notice, until such time that SBG's processing can be brought into compliance with those regulations. Moreover, any data that has been collected to data in contravention of those norms should be siloed and data subjects informed, so they can exercise their rights to have the data erased.

144. Given the widespread and systemic issues identified, the Commissioner should act with haste to mitigate the harms being caused.

145. The Commissioner will be aware of the development within the regulated gambling industry of the 'Single Customer View' initiative, and may already be considering the data protection implications of that initiative, whether by review

---

[32] In principle, a failure to comply with PECR in the sending of direct marketing material to a consumer without valid consent constitutes a breach of social responsibility code provision 5.1.11, which can be enforced as a condition of the operating licence (by section 82(1)) and so justify a licence review. However, the present issues are not directly concerned with that sort of PECR compliance, but with more fundamental and anterior questions of processing, the purpose of which is ultimately to send and target marketing material. Otherwise, controls on marketing are primarily concerned with ensuring that gambling marketing is not sent to a person who has sought to self-exclude (social responsibility code provision 3.5.3). Whilst some consumers vulnerable to gambljng addiction self-exclude, many do not, or do not do so in time.
[33] https://ico.org.uk/media/about-the-ico/documents/1560121/mou-gambling-commission.pdf

of a DPIA or otherwise. This Submission is not directly concerned with that initiative, but the Commissioner will wish to have regard to such developments – which increase the amount of, and ease with which, consumer personal data is to be processed by the gambling industry – when assessing the potential for impact on data subjects were the non-compliant and unlawful processing of SBG (and others like it) outlined here left unaddressed by the competent regulator. If the Commissioner would be assisted by Clean Up Gambling's more detailed comments on the Single Customer View initiative, Clean Up Gambling would be very happy to assist.

146. Clean Up Gambling are available to meet with the Commissioner and provide further evidence to any such investigation as the Commissioner may need.

Christopher Knight

11 KBW

Ravi Naik

Alexander Lawrence-Archer

AWO

24 June 2022