GENERAL DATA PROTECTION REGULATION (GDPR)

GUIDANCE FOR THE ONLINE GAMBLING INDUSTRY

Guidance is to help licensed online gambling operators to comply with their obligations under GDPR

www.rga.eu.com

GENERAL DATA PROTECTION REGULATION (GDPR): GUIDANCE FOR THE ONLINE GAMBLING INDUSTRY

Contents

Paragraphs

Guidance

1. The purpose of this guidance is to help licensed online gambling operators to comply with their obligations under GDPR. It is a first step towards a Code of Conduct for the sector once GDPR is fully implemented in 2018. Although providing some context it focuses on sector specific issues. As such it is not designed to provide detailed guidance or advice on every aspect of GDPR and, as ever, compliance is ultimately the responsibility of individual entities.

Codes of Conduct

2. Further information will be provided in due course by the relevant regulators. In the case of the UK, this is the Information Commissioners' Office (ICO) about the processes for submitting Codes for approval; their registration; and publication. However, Art 40 allows for 'representative bodies' to put in place

a Code of Conduct. The intention is that in due course this guidance will provide the basis for such a Code for the online gambling sector subject to it being submitted to the ICO for formal approval under Art 40 (5) and (6).

.

Background

3. An overview of the GDPR and associated requirements can be found at: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

4. It highlights the key themes of the General Data Protection Regulation (GDPR) to help organisations understand the new legal framework in the EU. It explains the similarities with the existing UK Data Protection Act 1998 (DPA), and describes some of the new and different requirements. It is for those who have day-to-day responsibility for data protection.

5. It will be reviewed and updated as necessary. The GDPR will apply in the UK from 25 May 2018.

6. Many third parties have published their own guides to GDPR and these can be useful sources of information. The RGA does not endorse any of them, but examples include:

- https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en

- http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

- http://www.lawsociety.org.uk/Support-services/Practice-management/GDPR-preparation/general-guidance-on-gdpr/

- http://www.ucl.ac.uk/legal-services/guidance/dp_GDPR

Accountability and governance

7. The ICO guidance states that: *'The accountability principle in Article 5(2) requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.'*

8. Although complying with a principle presents practical challenges this provision is a starting point for much of what follows.

9. Companies, according to the ICO, will be '*expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are now legally required in certain circumstances.*

Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many organisations will already have good governance measures in place.'

10. Against this background all operators should have in place internal processes that demonstrate a commitment to these principles. These should include general policies (ie on lawful processing); where responsibilities lie within the company structure for DP and GDPR compliance; and structures for recording and monitoring related decisions and structures.

When is a Data Protection Officer (DPO) required?

11. Further advice on this is due to be published by the ICO. In the meantime it is worth noting the EU Article 29 Working Party guidelines (see http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360) and the fact that Article 37(1) of the GDPR sets out three cases in which a DPO must be appointed:

    1. where the processing is carried out by a public authority or body (except courts acting in a judicial capacity);

    2. where the core activities of the controller or of the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or,

    3. where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Data protection impact assessments (DPIA)

12. Another building block in preparing for and applying the new GDPR requirements are Data protection impact assessments (also known as privacy impact assessments or PIAs). The ICO describes them as 'a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.'

13. Further information can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Lawful basis for processing personal data

14. The lawful bases to justify the processing of personal data are where:

- there is a **legal obligation** to do so (ie if there is a need to process the personal data to comply with a common law or a statutory obligation);
- **consent** has been given by the data subject;
- there is a **legitimate interest** in doing so (this needs to be balanced with the rights and freedoms of the data subject);
- it is required by **contract;** and
- it is a **vital interest** (ie of the data subject or another natural person and generally refers to a life threatening situation) or a **public task** (ie when the processing is necessary for a task carried out in the public interest).

15. Further information can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

16. The two other areas are of importance to the sector and are more open to interpretation. Consequently the next two sections of this guidance go into more detail on **consent** and **legitimate interest.**

17. Finally, it should be remembered that for many of the lawful bases, a necessity test needs to be met (eg necessary for performance of a contract, necessary for compliance with a legal obligation, necessary for the purposes of legitimate interests) before they can be relied upon.

Consent

18. The definition of consent is “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”

19. Consent given by individuals to the use of their data for clearly defined purposes remains an option under GDPR, but the changes brought forward by GDPR constitute a tighter regime for the use of ‘consent’. New factors, subject to additional guidance from the ICO, to consider are that the data subject must have the right to withdraw consent at any time; and the consent will not be valid unless separate consents are obtained for different processing activities.

20. The way in which consent is sought is also changing. The main changes to note are that:

    - It must be separable from other written agreements, clearly presented and as easily revoked as given.

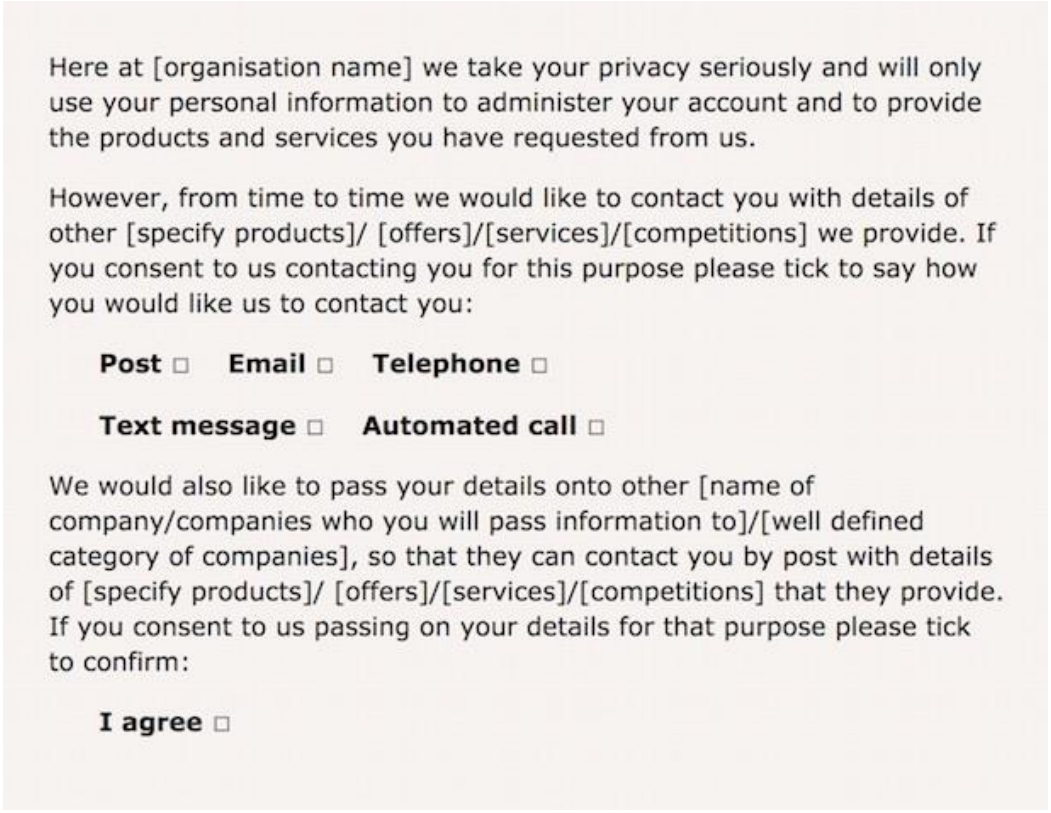
    - Consent must be active rather than passive (no pre-ticked boxes, consent being applied without specific agreement etc)

    - Non-consent to processing which is not necessary for the service being supplied cannot be used to justify suspension of that service.

    - The terms of consent and the way to withdraw consent at any time should be set out clearly (this would normally be contained in privacy notices). The current ICO guidance also states that this should ‘*Be*

specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.'

21. When seeking consent companies should explain to the data provider/subject exactly what they are agreeing to and in a form they can reasonably be expected to understand. The language should be clear and unambiguous. The following is an example:



Here at [organisation name] we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.

However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:

Post □ **Email** □ **Telephone** □

Text message □ **Automated call** □

We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you consent to us passing on your details for that purpose please tick to confirm:

I agree □

22. There is no provision for any form of implied consent. Similarly 'silence' or 'inaction' cannot be interpreted as consent and there is a requirement that consent be 'demonstrable'.

23. With regard to the period for which consent can be deemed to last, the ICO's consent guidance says "There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

24. For the online gambling sector it will be rare for consent to be sought where children are concerned but should it occur then verifiable parental consent is required. It should also be noted that for direct marketing, the Privacy and Electronic Communications Regulations (PECR) require consent for marketing by certain channels. PECR will apply alongside GDPR until replaced by the EU ePrivacy Regulation.

Legitimate interests

25. It is very clear that where a company relies on this test the legitimate interests cited must be clear and objectively justifiable.

26. Legitimate interests can be defined broadly, but examples given in the GDPR Recitals (see https://gdpr-info.eu/recitals/) include:

    • Recital 47: processing for direct marketing purposes or preventing fraud;

    • Recital 48: transmission of personal data within a group of undertakings for internal administrative purposes, including client and employee data (note international transfer requirements will still apply – (see section on transfers of personal data);

    • Recital 49: processing for the purposes of ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems; and

    • Recital 50: reporting possible criminal acts or threats to public security to a competent authority.

27. The caveat to this is that although these purposes are mentioned in the recitals, this does not necessarily mean that they will always constitute a legitimate interest. Ultimately, it is for the data controller to demonstrate the legitimate interest and the balancing act with data subjects' rights and freedoms.

28. The expectations of data subjects must also be taken into account when assessing whether their legitimate interests outweigh the interests of the data controller. The Recitals state that the interests and fundamental rights of data subjects '*could in particular override*' that of the controller where data subjects "*do not reasonably expect further processing*."

29. Privacy notices must now set out the legitimate interests where they are relied upon in relation to specific processing operations. Legitimate interest is open to a broad interpretation for data processing and profiling purposes.

30. Although the obligation to demonstrate legitimate interest must rest with the data controller, in the online gambling industry legitimate interest could include:

    - Combating crime (eg anti-fraud, anti-money laundering etc) which could also include legal obligations, for instance, under money laundering regulations and legislation.

    - Provision of services (account creation, account functionality, access to gambling, payment processing etc)

    - Commercial (eg marketing, personalisation of offers, VIP management, trading decisions, credit worthiness, promotions and bonuses, loyalty programmes, value profiling and risk management such as promotional controls & stake factoring)

- Social responsibility (eg minimisation of gambling related harm)

- Safeguarding the integrity of sports (ie unusual or suspicious betting patterns that could indicate a threat to the integrity of an event)

- Regulatory and statutory requirements (eg potentially any of the above categories, such as combating crime, plus specific know-your-customer issues such as location, device used etc which might be needed to comply with the Gambling Commission's Licence Conditions and Codes of Practice.)

31. It follows that in every case where legitimate interest is applied that each company should maintain a log which records the basis on which any assessments have been made. This is good practice in any event, but data processed on the basis of legitimate interests is subject to a right to object and the decision log will provide a basis for withstanding that or other potential challenges.

32. With regard to any objections, the burden lies with data controllers to prove they have compelling grounds to continue processing the data. If they fail to do so it can lead to the exercise of rights to restrict and erase data**.**

33. As is the case when seeking consent (see above), when giving details of the grounds for processing (ie consent, contractual, legitimate interests, legal) it should be explained in customer friendly language rather than in the technical language used by GDPR.

Privacy notices

34. GDPR states that the information companies must provide about personal data processing should be:

- concise, transparent, intelligible and easily accessible;

- written in clear and plain language, particularly if addressed to a child; and

- free of charge (although in the case of a privacy notice this is a moot point).

35. An example of this can be found at https://iapp.org/about/privacy-statement/:

36. For further details the following ICO guidance should be considered: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

Security: Pseudonymisation and Anonymisation

37. Pseudonymisation and anonymization have been grouped here under the more general heading of ‘security’ but it is necessary to have a clear understanding of the distinction between the two.

38. Recital 26 of the GDPR clarifies that **pseudonymised** data is that which can be attributed to a natural person, which when combined with additional information (often referred to as “key” in the case of encrypted or hashed data) results in them becoming identifiable.

39. If the data does not relate to an identifiable natural person, or if from the information the person is no longer identifiable, then the information is considered to be **anonymised.** This means that if the data truly is anonymised then the processing of it is seen to fall outside of the provisions of the GDPR. In such circumstances, data controllers would be required to demonstrate that the data is truly anonymised and that no means exist by which individuals could be re-identified, either by the data controller or another organisation.

40. Even in this form it still constitutes personal data, however it can still be used in certain situations. These could include:

    - Whether it is a factor to be considered when determining if processing is “incompatible” with the purposes for which the personal data was originally collected and processed;

    - Where it is included as an example of a technique which may satisfy requirements to implement “privacy by design and by default”;

    - When it may contribute to meeting the GDPR’s data security obligations; and

    - Circumstances where the data is to be used for research.

41. It would be good practice for all companies to develop internal pseudonymisation and anonymization standards to improve consistencies of approach. As with much else these should be prepared in the light of current and emerging guidance from the ICO.

42. More generally with regard to security and information security it should be noted that minimum standards are already required under various regulations (for example, all operators licensed by the British Gambling Commission are required to comply with a sub-set of ISO27001 through annual security audits). These constitute minimum standards and many operators can and do adhere to higher standard.

Profiling

43. Profiling is defined in GDPR as *any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict certain aspects concerning that natural person’s performance at work, economic situations,*

health, personal preferences, interests, reliability, behaviour, location or movement.

44. With regard to automated decision-taking which includes, but is not limited to, profiling, attention should be given to the following rules:

    - They apply where the decision produces legal effects or has similarly significant effects (ie Recital 71 gives the example of online credit decisions and e-recruiting)

    - Article 22 places a prohibition on solely automated decision making, but there are scenarios where that Article 22 right does not apply. These would be where the decision is necessary for the entry into or performance of a contract; or − authorised by Union or Member State law applicable to the controller; or − based on the individual's explicit consent then automated processing can be used. However, suitable measures to protect the individual's interests must still be in place.

    - There are additional restrictions on profiling based on sensitive data – which need explicit consent, or to be authorised by Union or Member State law which is necessary for substantial public interest grounds. In the UK this would require data controllers to satisfy a substantial public interest condition under Schedule 1 of the Data Protection Bill (which it is assumed will remain when that Bill becomes law in 2018).

    - Data relating to children is especially sensitive.

    - If automated decision-taking is based on consent, then (see section above) that consent must be explicit. Also, in line with WP29 guidance, any manual intervention in the processing must be meaningful, and cannot simply be introduced to circumvent the rule regarding processing being 'wholly automated'.

45. Article 13 (1) requires that where personal data relating to a data subject are collected from the data subject, the controller shall, at a time when personal data are obtained, provide the subject with the information including:

    - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; and

    - the legitimate interests pursued by the controller or third party.

    - It is sufficient that this information is set out clearly in a disclosure statement (privacy policy) rather than T&Cs and this should be the "earliest instance" rather than at the time of profiling.

    - Article 13(2)(f) also requires data controllers to provide information on the existence of profiling including meaningful information about the logic involved and the significance and envisaged consequences.

46. When this information is provided data subjects should also be made aware that they have a right:

    - to challenge the use of profiling, especially where the justification is legitimate interest (Art 21);

    - to demand the opportunity to make representations and for human intervention (Art 22); and

    - impact assessments have to be carried out where profiling will have significant legal effects on the individual (Art 35)

Human intervention

47. The Recitals and the GDPR make an explicit distinction between purely automated decision-taking and that where there is an element of human intervention on the process. The degree of human intervention that would satisfy this requirement is largely untested. However, in the online gambling sector where profiling is a demonstrable necessity to meet various regulatory requirements (for example to combat money laundering or fulfil player protection obligations) then it is anticipated that the vast majority of key decisions would already require some notable degree of human intervention in order for a decision to take place.

Special category data

48. If personal data is being used which the GDPR defines as 'special categories' then particular care should be paid. These categories are racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition; sexual life, the commission or alleged commission by the data subject of any offence; or any proceedings for any offence that are currently ongoing. Article 10 of the GDPR should be referred to for more details. Although it would be comparatively rare for operators in the online gambling sector to hold or utilise special category data there might be instances where it does so (for example, where a Power of Attorney is used with supporting medical evidence to advise an operator that a customer is no longer capable of making informed decisions or managing their gambling accounts for themselves; where there are potential links between problem gambling and mental health; or where there is information relating to alleged or confirmed offencds) and there should be clear internal and compliant processes for dealing with those situations when they arise.

49. More information about the conditions for processing can be found in Article 9 and data controllers will also need to be aware of the conditions under Schedule 1 of the Data Protection Bill that cover substantial public interest processing of special category data and processing of criminal offence/conviction data.

Portability

50. Subject access rights and requests are longstanding provisions, but GDPR goes further and requires the controller to provide information in a structured, commonly used and machine readable form so that it may be transferred by the data subject to another data controller without hindrance. There is therefore an overlap here between the right to be informed and the right to data portability, but they remain two separate rights.

51. Where it is possible the controller can be required to transmit the data directly to another controller and the GDPR encourages controllers to develop interoperable formats. This might be a longer term objective for the online gambling sector, but it is not currently an option. However, it is suggested that controllers state in their initial post-May privacy policies that this is a longer-term objective but is not yet possible within the sector. This guidance will be updated and amended accordingly as and when an agreed model can be implemented.

52. Portability applies (see Recital 68) to:

    a. personal data which is processed by automated means (no paper records);

    b. personal data which the data subject has provided to the controller; and

    c. where the basis for processing is consent, or that the data are being processed to fulfil a contract or steps preparatory to a contract.

53. However, the portability right does not extend to personal data which is inferred or derived by the data controller (for example, the results of an algorithmic analysis of an individual's behaviour). This is an especially complex area and companies will wish to take into account the Article 29 Working Party guidance on portability and might wish to seek specialist legal advice if deciding to rely on this provision.

54. For the online gambling sector regulatory requirements compel companies, subject to Data Protection Act safeguards, to hold a wide range of data about their customers. These would commonly relate to areas where such information is required to manage accounts adequately to combat crime and problem gambling behaviour. In addition there are legitimate interests that justify additional profiling for commercial reasons; and information which is commercially sensitive or disproportionate (eg a list of every bet placed by a customer). None of these types of information would normally form part of any data provided under the portability provisions, but ultimately this is for the data controller to determine..

Right to be forgotten and retention

55. Customers have the right to have their data 'erased' in certain specified situations. This is in essence where the processing fails to satisfy the requirements of the GDPR. Where customers seek to exercise these rights, data controllers must respond without undue delay (and in any event within one

month). This period can be extended in difficult cases, but data controllers would need to demonstrate their justification for relying on the extension provision.

56. Situations where the right applies are:

> • When data are no longer necessary for the purpose for which they were collected or processed.
>
> • If the individual withdraws consent to processing (and if there is no other justification for processing).
>
> • Where there are no overriding legitimate interest grounds and the individual exercises their right to object – ie where the individual objects and the controller cannot demonstrate that there are overriding legitimate grounds for the processing. In the online gambling sector, one of these grounds would be where a customer has self-excluded and then perhaps seeks to rely on the right to be forgotten in order to circumvent that exclusion; it would be a legitimate ground not to comply with the request because there is a legitimate interest in maintaining high social responsibility standards and compelling the customer to abide by the terms of their self-exclusion.
>
> • When the data are otherwise unlawfully processed (i.e. in some way which is otherwise in breach of the GDPR or other legislation).
>
> • If the data have to be erased to comply with Union or Member State laws which apply to the controller (ie online gambling is likely to fall within the definition of information society services referred to in Article 17(1)(f)

57. Where a controller is obliged to erase the data, but that data has already been put into the public domain or shared with other controllers, then the controller must also inform other controllers who are processing the data that the data subject has requested erasure of those data.

58. Aside from the right to be forgotten, Article 5 (e), reflects the existing requirements under the Data Protection Act, and states that personal data should 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the individual.'*

Rights of the data subject

59. Chapter Three of the GDPR (see https://gdpr-info.eu/chapter-3/) sets out in one place references to the twelves Articles which contain provisions about the rights of the data subject. Regard should be had to these articles when developing internal compliance procedures and when dealing with queries from data subjects.

Definitions

60. In the interests of consistency the objective must be wherever possible to have agreed definitions of key terms. There will be some common themes across all regulations and guidance, but Annex A includes a number which will be specific to the online gambling sector.

ANNEX A

DEFINITIONS

Data subject – the data subject is the person the data is about. It is an identifiable person who can be identified by an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to person's physical, physiological, genetic, mental, economic, cultural or social identity

Data controller – A person or body, alone or jointly, which determines the purposes and means of processing personal data

Data processor – the data processor carries out specific tasks on behalf of the data controller under contract and is generally not liable for enforcement if it does what it is told to do by the data controller.

Personal data - any information relating to an identified or identifiable, either directly or indirectly, natural person (a natural person is an individual rather than a legal person like a company)

Data Protection Directive - The European Directive 95/46/EC previously governed the processing of personal data in the EU and will now be replaced by the GDPR

DPO A Data Protection Officer – whose appointment is obligatory under the GDPR where: (i) processing is carried out by a public authority; or (ii) the "core activities" of a data controller / data processor either: (a) require "the regular and systematic monitoring of data subjects on a large scale" or; (b) consist of processing of special categories of data or data about criminal convictions "on a large scale".

GDPR The General Data Protection Regulation - adopted as Regulation (EU) 2016/679 on 27 April 2016.

Pseudonymisation - The technique of processing personal data so that it can no longer be attributed to a specific individual without the use of additional information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

Right to be forgotten - The data subject's existing right to deletion of their personal data, in certain circumstances, has been extended to a new 'right of erasure' in circumstances detailed in Chapter III Section 3 GDPR.

Subject access - This is the data subject's right to obtain from the data controller, on request, certain information relating to the processing of his/ her personal data as detailed in Chapter III Section 2 GDPR.

Profiling – the use of automated techniques to "evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that

natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.