6 December 2017 **DPB (17–19) 001**

JOINT COMMITTEE ON HUMAN RIGHTS

NOTE FROM DEPUTY COUNSEL

THE HUMAN RIGHTS IMPLICATIONS OF THE DATA PROTECTION BILL

I. Introduction

1. The Data Protection Bill (*hereinafter* 'the Bill') was introduced in the House of Lords on 13 September and will proceed to Report stage on 11 December. This Note outlines the significant human rights issues raised by the Bill for the Committee's consideration. The Committee has received written evidence from six organisations whose submissions are incorporated into this Note.[1]

2. This Note is structured as follows:
   a) Section II sets out a summary of the Convention rights engaged by the Bill and an overview of the human rights concerns that arise in respect of the right to privacy and data protection;[2] the right to freedom of expression;[3] the right to be free from discrimination;[4] and the right to a fair trial.[5]
   b) Section III provides an overview of the data protection legal framework set out in the EU General Data Protection Regulation (*hereinafter* 'the GDPR') and the Bill;
   c) Section IV sets out some of the key human rights issues that arise in the Bill, namely:
      i. The omission of Article 8 of the Charter of Fundamental Rights from the Bill;
      ii. The broad exemptions from data rights and principles permitted for:
         - immigration control;
         - the right not to be subject to automated decision-making;

[1] To be published on 6 December 2017 on JCHR's website. The organisations that submitted evidence are: Amnesty International, The Equality and Human Rights Commission, Liberty, MedConfidential, Open Rights Group, and Privacy International.
[2] Article 8 of the European Convention on Human Rights (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the EU
[3] Article 10 ECHR
[4] Article 14 ECHR
[5] Article 6 ECHR

- special categories of data (i.e. sensitive data);[6]
- cross-border transfers of data;
- national security certificates;
- intelligence services; and
- freedom of expression purposes.

iii. Delegated powers permitting Ministers to add further exemptions that could alter individuals' rights without parliamentary scrutiny;

iv. Reverse burdens of proof in relation to data offences and limitations on the right to bring claims for data breaches;

v. The low age of consent for children in accessing online services.

d) Section V suggests points of further consideration for the Committee.

3. The Bill is complex and raises a number human rights concerns. The Committee may wish to explore some of these issues further. In sum, the key questions for the Committee's consideration are as follows:

a) whether Article 8 of the Charter ought to be expressly included in the Bill;
b) whether an exemption for effective immigration control is necessary and proportionate given the broad reach this exemption would have;
c) whether automated decision-making requires further safeguards to ensure that decisions significantly affecting human rights are not being made on an automated basis;
d) whether the Bill provides sufficient clarity as to the meaning of "substantial public interest" and "public interest" and whether the safeguards for processing of "special categories data" are sufficient;
e) whether the powers contained within the Bill permitting cross-border transfers of data and the unfettered powers granted to the intelligence services in the absence of any safeguards are necessary and proportionate;
f) whether the broad and indefinite national security exemptions are necessary and proportionate and whether oversight for the issuing of national security certificates is sufficient;
g) whether the right of appeal against national security certificates provides an effective judicial remedy;
h) whether the significantly reduced safeguards for intelligence services are necessary and proportionate and whether there is sufficient oversight of the intelligence services given their broad and unfettered powers;

[6] "Special categories of data" are defined in Article 9: 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.

i) whether to engage with the Intelligence and Security Committee and the Independent Reviewer of Terrorism Legislation to explore further the matters concerning national security;
j) whether the delegated powers are necessary and proportionate in light of the breadth of the powers and the potential to remove rights without parliamentary scrutiny;
k) whether the reverse burdens constitute a proportionate interference with Article 6(2) ECHR and whether a broader defence to the new 're-identification' offence is required;
l) whether civil society organisations ought to be empowered to bring complaints and seek effective remedies in the public interest; and
m) whether the age of consent complies with the best interests of the child principle.

II. Summary of human rights implications

4. This Bill primarily engages with four Convention rights: the right to privacy and family life (Article 8); the right to freedom of expression (Article 10); the right to be free from discrimination (Article 14); and the right to a fair trial (Article 6). The analysis that follows focuses predominantly on the extent of the Bill's compliance with these Convention rights, as well as Article 8 of the EU Charter of Fundamental Rights. Lord Ashton of Hyde has made a statement of compatibility under section 19(1)(a) of the *Human Rights Act 1998*. The Government has not published an ECHR memorandum instead relying upon the human rights analysis set out in the Explanatory Notes.[7]

5. With the exception of Article 6,[8] these rights are qualified and may be restricted for legitimate aims where necessary and proportionate.[9] Whilst the Bill, in some respects, is 'rights-enhancing', it provides numerous exemptions and derogations that serve to exclude fundamental rights and principles in certain circumstances. The key question is whether the Bill strikes the appropriate balance between competing rights and interests. As stated by Lord McNally in the course of Second Reading debate: "the elephant in the room always in discussing a Bill such as this is how we get the balance right between protecting the freedoms and civil liberties that underpin our functioning liberal democracy while protecting that democracy from the various threats to our safety and well-being."[10] This Note considers the main provisions of the Bill that engage Convention rights, bearing in mind that any

[7] Correspondence between Deputy Counsel and Department for Culture, Media, and Sports. See Explanatory Notes (EN), paras 802 – 818
[8] Article 6 is not qualified but it is limited, i.e. it can be restricted in explicit/finite circumstances set out in the article itself or restrictions implied by the European Court of Human Rights. See Blackstone's Guide to the Human Rights Act 1998, 2011, OUP, Chapter 2, para 2.28
[9] Article 8(2), Article 10 (2)
[10] Second Reading debate, HL, 10 October 2017, Hansard Vol. 785, col. 135

interference with such rights much be in accordance with the law,[11] necessary in a democratic society,[12] and proportionate as required by human rights law.[13]

The rights to privacy and data protection

6. The Bill predominantly engages the rights to privacy and data protection, which are incorporated into domestic law by the *Data Protection Act 1998* (DPA) and the *Human Rights Act 1998* (HRA), and contained in Articles 7 and 8 of the Charter. Article 8 of the Convention states that "everyone has the right to respect for his private and family life, his home and his correspondence." The threshold for engaging Article 8 is low.[14] The state is under a negative obligation not to interfere with privacy rights and a positive duty to take measures to prevent private parties from interfering with these rights.[15] The scope of Article 8 ECHR includes the protection of personal data and requires the law to provide safeguards ensuring that data is relevant and not excessive; that data is held for no longer than necessary; and that retained personal data is protected from misuse and abuse.[16] These principles are reflected in the GDPR and the Bill.[17] In certain circumstances, Article 8 ECHR protects the right not to have private information retained by the state or disclosed to third parties.[18] It also imposes a positive obligation on the state to provide copies of stored personal information unless there are compelling reasons for refusing.[19]

7. Article 8 ECHR is a qualified right. Any interference must be in "in accordance with the law", necessary in a democratic society in pursuit of one of the legitimate aims set out in Article 8(2).[20] For an interference to be "in accordance with the law", it must be "compatible with the rule of law", include a "measure of legal protection against arbitrary interferences by public

[11] There must be a specific legal rule or regime which authorises the interference; the individual must have adequate access to the law in question (*The Sunday Times v United Kingdom* (1979) 2 EHRR 245); and the law must be formulated with sufficient precision to enable the citizen to foresee the circumstances in which the law would or might be applied (*Malone v United Kingdom* (1984)7 EHRR 14).
[12] Necessity requires that an interference corresponds to a pressing social need and that it is proportionate to the legitimate aim pursued.
[13] If a measure has been adopted which infringes an individual's Convention right in some way, it will not be considered disproportionate if it is restricted in its application and effect, and is duly attended by safeguards in national law so that the individual is not subject to arbitrary treatment (*MS v Sweden* (1997) 3 BHRC 248).
[14] *London Borough of Harrow v Qazi* [2003] UKHL 43, [2004] 1 AC 983, at paras 8-10
[15] *(1) X (2) Y v the Netherlands* (1985) 8 EHRR 235
[16] *S and Marper v UK* (Grand Chamber) 4 December 2008, Applications nos. 30562/04 and 30566/04
[17] Article 5, GDPR
[18] Blackstones Guide to the Human Rights Act, OUP, 2011, p238, para 7.274
[19] *Ibid.*
[20] These are: national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals; or for the protection of the rights and freedoms of others.

authorities", and prescribe with "sufficient clarity" the scope of any discretion conferred.[21] The principle of proportionality is key to the interpretation of data protection legislation,[22] particularly where fundamental rights are in play.[23] The degree of scrutiny applied by the courts when assessing the proportionality of interferences under Article 8(2) will turn on the facts of the case and the nature of the rights at stake.[24]

8. Articles 7 and 8 of the Charter also protect these rights and go beyond the protections offered by the Convention. Article 7 of the Charter reflects Article 8 of the ECHR, except that "correspondence" has been changed to "communications" to take account of changing technology. Article 8 of the Charter sets out the right to protection of personal data, which must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Article 8 of the Charter also provides that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

9. Whilst the aim of the Bill is to enhance privacy and data protection rights, it contains numerous exemptions or derogations from fundamental data rights and principles. Whilst many of these may be justified, a number of the exemptions appear to be an unnecessary and/or disproportionate interference with privacy rights. The following exemptions are of particular concern:
    i. the exemptions permitted on the grounds of "effective immigration control";
    ii. the exemptions from the right not to be subject to automated decision-making;
    iii. the exemptions from the prohibition of processing special categories of data;
    iv. the exemptions permitting cross-border transfers in the public interest;
    v. the exemptions permitted by national security certificates;
    vi. the exemptions permitted for the intelligence services;
    vii. the exemptions permitted for the purpose of freedom of expression.

10. Further, despite the wide-ranging exemptions provided for in the Bill, the Secretary of State is given broad delegated powers to add further exemptions.

[21] *Gillan v UK* (2010) 50 EHRR 45 paras 76-77 and *Weber and Saravia v Germany* (2009) 46 EHRR SE5 at paras 93-94.
[22] *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74; [2017] 1 W.L.R. 3255 and *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd* [2017] EWCA Civ 121; [2017] 3 W.L.R. 811
[23] *Pham v Secretary of State for the Home Department* [2015] UKSC 19; [2015] 1 W.L.R 1591.
[24] Blackstones Guide to the Human Rights Act, OUP, 2011, p238

Consequently, rights to privacy and data protection could be eradicated in certain circumstances without effective parliamentary scrutiny.

The right to freedom of expression

11. The rights to privacy and data protection must be balanced with the right to freedom of expression and the right to receive and impart information protected by Article 10 of the ECHR. This includes the right to receive information that the State holds about citizens.[25] Both Articles 8 and 10 of the Convention must be given effect in a non-discriminatory manner. Concerns have been raised as to the balance struck between Article 8 and Article 10, given the exemptions permitted for "special purposes" including journalism.

The right to be free from non-discrimination

12. Article 14 ECHR requires that the enjoyment of the rights and freedoms set out in the Convention must be secured without discrimination "on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth, or other status." This is not a free-standing right, rather it requires that Convention rights are secured in a non-discriminatory fashion. Where exemptions or derogations to rights engage Article 8 or 10 in a discriminatory manner, Article 14 will also be engaged. The exemption for immigration control therefore raises issues under Article 8, Article 10, and Article 14, given its likelihood to disproportionately affect non-British individuals.

The right to a fair trial

13. Article 6 ECHR guarantees the right to a fair trial, which includes the presumption of innocence. Firstly, this right is engaged by the various offences and defences provided for in the Bill, as well as the provisions setting out rights of challenge and appeal. There are numerous criminal offences set out in the Bill, including new offences. Many of the defences reverse the burdens of proof (putting the onus on the defendant to "prove" his defence[26]), engaging the presumption of innocence. Secondly, national security certificates (issued by the Secretary of State) may only be appealed on judicial review principles and are unlikely to be disclosed, thereby precluding any possibility of challenge. Thirdly, civil society organisations are prohibited from bringing a challenge unless they are instructed by a litigant. These provisions may interfere unjustifiably with Article 6.

The rights of the child

14. Finally, in both domestic law and international law, the UK has obligations to protect the rights of the child, including giving paramount importance to the

[25] *Leander v Sweden*, ECtHR, 26 March 1987, Series A No.116
[26] Clauses 139, 160, 163, and 171 of the Bill

best interests of the child.[27] The Bill sets the age of consent for children to access online services at 13, which is the lowest age permitted by the GDPR. Concerns have been raised that this age has been set without any evidence or consultation to justify this decision.

III. Overview of the data protection legal framework

15. The Bill is shaped by the EU legal framework on data protection, which currently underpins the UK's domestic law and ensures the flow of data between the UK and other states. In January 2012, the European Commission proposed a new legislative framework for data protection which consisted of the General Data Protection Regulation ('GDPR')[28] and the Law Enforcement Directive.[29] In addition to these two instruments, UK data protection law is also shaped by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Articles 7 and 8 of the EU's Charter of Fundamental Rights. The Bill provides that domestic data protection law will be governed by the GDPR, the 'applied GDPR' (post-exit),[30] the Bill, and any regulations made under the Bill.[31]

The GDPR

16. The GDPR came into force on 24 May 2016 and will have direct application in Member States. The GDPR will apply in the UK from 25 May 2018[32] and will be incorporated into domestic law as part of "retained EU law".[33] The GDPR sets out the responsibilities of "data controllers"[34] and "data processors"[35] as well as the rights of "data subjects"[36] within the scope of EU law. It applies to processing by organisations within the EU and those outside the EU offering goods and services in the EU.[37] It will have extra-territorial effect such that wherever an EU citizen's data is being processed, the GDPR rules will apply.[38]

[27] Children Act 1989; U.N. Convention on the Rights of the Child 1989
[28] The GDPR will apply in the UK from 25 May 2018 and will be retained in domestic law post-exit day by virtue of the EU (Withdrawal) Bill.
[29] The Law Enforcement Directive must be transposed into national law by 6 May 2018.
[30] I.e. it applies outside of the scope of Union law.
[31] Section 2(9)(a)-(e) of the Bill
[32] There is a two-year transition period for implementation.
[33] Clause 3, EU (Withdrawal) Bill
[34] The bodies that determine the purposes and means of processing of personal data
[35] Those who process personal data on behalf of a controller
[36] The individuals whose personal data is being processed
[37] Article 3(2) GDPR. For further discussion see Commons Library Briefing Paper, Brexit and Data Protection, 10 October 2017, p6
[38] *Ibid.*

17. The GDPR applies to “personal data”, which has a wider definition than under current law:

> “Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.”[39]

18. This means that more types of data will be within the scope of the Bill than under the current DPA. “Special categories of personal data” (“sensitive personal data” under the current DPA) is also widened to include genetic and biometric data.[40] Criminal conviction data is dealt with as a separate category of data with extra safeguards.[41]

19. The fundamental principle underlying the GDPR (and the Bill) is that data can only be processed where a lawful basis is identified. The lawful basis will affect the rights of the data subject, for example, where the processing is based on consent, the individual will be able to exercise stronger rights such as the right to have their data deleted.[42] Article 6(1) of the GDPR provides the following bases for lawful data processing:
    a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
    b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    c) processing is necessary for compliance with a legal obligation to which the controller is subject;
    d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[43]

---

[39] Article 4 GDPR
[40] Article 9(1) GDPR
[41] Article 10 GDPR
[42] Information Commissioner’s Office, *Overview of the GDPR*, 20 October 2017, p9
[43] Article 6(1) GDPR. Basis (g) is not applicable to public authorities in the performance of their duties - Article 6(2) GDPR.

20. There are specific conditions for "special categories of data" that must be satisfied in addition (discussed below at paragraphs 56 - 60).

Data protection principles

21. The GDPR sets out a series of data protection principles[44] and rights,[45] which are replicated in the Bill. The data controller is responsible for ensuring that data processing is:
    a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
    b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;[46]
    c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
    d) accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay;
    e) 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;[47]
    f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[48]

Data protection rights

22. Data subjects will have the following rights in relation to their personal data, subject to various exemptions and derogations.

    Right to be informed

23. The right to be informed encompasses the obligation to provide "fair processing information", typically through a privacy notice, and requires transparency as to the use of personal data. [49] Information provided to

[44] Article 5 GDPR
[45] Articles 12-22 GDPR
[46] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.
[47] 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.
[48] Article 5 GDPR
[49] Articles 12(1), 12(5), 12(7), 13 and 14 and Recitals 58-62 GDPR. For further details on each of these rights see Information Commissioner's Office, *Overview of the GDPR*, 20 October 2017.

individuals must be concise, transparent, intelligible, accessible, clear, and free of charge.[50]

Right of access

24. Data subjects will have the right to obtain confirmation from a data controller as to whether or not their personal data is being processed, where and for what purpose, and access to their personal data. A subject access request (SAR) will no longer be subject to a fee (unless the request is manifestly unfounded, excessive or repetitive). Data controllers must provide information without delay and within one month or receiving the request. A refusal to comply with a SAR must be accompanied by explained reasons and information regarding the complaints and remedies.[51]

Right to rectification

25. Data subjects will be entitled to have their personal data rectified if it is inaccurate or incomplete. Where data controllers have disclosed personal data to third parties, they must inform the third parties of the rectification where possible, as well as notifying the data subjects of such disclosure. Data controllers must comply with requests for rectification within one month (or two if complex).[52]

Right to erasure

26. The right to erasure (or the right to be forgotten) gives data subjects the right to request the erasure of personal data where there are no compelling reasons for continued processing. This is not an absolute right and will only apply in specific circumstances:
    a) the data is no longer necessary in relation to the original purposes for processing;
    b) the data subject withdraws consent;
    c) there is no overriding legitimate interest for continuing the processing;
    d) the data was unlawfully processed;
    e) the data must be erased to comply with a legal obligation;
    f) the data is processed in relation to the offer of 'information society services' to a child.[53]

27. The right is particularly relevant with respect to children, where a child has given consent to processing and subsequently requests erasure of their data.[54]

[50] *Ibid.*
[51] Article 12, 15, and Recital 63 GDPR
[52] Articles 12, 16, 19 GDPR
[53] Articles 17, 19, Recitals 65 and 66
[54] See Recital 65

28. Under the current DPA the right to erasure is subject to a threshold test – the data processing must have caused unwarranted and substantial damage or distress to the individual. There is no threshold test under the GDPR. However, the right does not apply if processing is necessary for the following reasons:
    a) freedom of expression or information;
    b) to comply with a legal obligation, or the performance of a public interest task, or the exercise of official authority;
    c) public health in the public interest;
    d) archiving purposes in the public interest, scientific research, historical research, or statistical purposes; or
    e) the defence of legal claims.[55]

Right to restrict processing

29. Individuals have the right to restrict the processing of their personal data in certain circumstances. Data controllers must restrict processing (and inform third parties) where:
    a) an individual contests the accuracy of the personal data and the accuracy is being verified;
    b) an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and consideration is being given as to whether the organisation's legitimate grounds override those of the individual.
    c) processing is unlawful and the individual opposes erasure and requests restriction instead;
    d) the controller no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.[56]

Right to object to processing

30. Individuals have the right to object to:
    a) processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
    b) direct marketing (including profiling); and
    c) processing for purposes of scientific/historical research and statistics.

31. Individuals must be informed of their right to object at the point of first communication. This must be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information. If the individual has an objection based on "grounds relating to his

[55] Article 17(3) GDPR
[56] Articles 18 and 19 and Recital 67 GDPR

or her particular situation", controllers must stop processing the personal data unless:

a) they can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
b) the processing is for the establishment, exercise or defence of legal claims.

32. If the data is processed for direct marketing purposes, there are no grounds of refusal. Conversely, if the data is processed for research purposes in the public interest, the objection can be refused.[57]

Right to challenge automated decision making and profiling

33. The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. Individuals have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the individual.[58] However, the right does not apply if:
    a) the decision is necessary for entering into or performance of a contract between the individual and the data processing organisation;
    b) is authorised by law (so long as the data subject's rights, freedoms and legitimate interests are safeguarded);[59] or
    c) based on explicit consent.[60]

34. Processing data for profiling purposes[61] is subject to various safeguards. When using data for profiling, organisations must:
    a) ensure processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences;
    b) use appropriate mathematical or statistical procedures for the profiling;
    c) implement appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors; and
    d) secure personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.[62]

[57] Articles 12, 21 and Recitals 69 and 70 GDPR
[58] Article 22 GDPR
[59] Article 22(2)(b) GDPR
[60] Article 9(2) GDPR
[61] The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict their: performance at work; economic situation; health; personal preferences; reliability; behaviour; location; or movements.
[62] Articles 4(4), 9, 22 and Recitals 71 and 72 GDPR

35. Further, automated decisions must not concern a child or be based on the processing of "special categories of data"[63] unless the controller has the explicit consent of the individual or the processing is necessary for reasons of substantial public interest on the basis of EU or Member State law. When processing for reasons of substantial public interest, this must be proportionate to the aim pursued, respect the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and the interests of the individual.[64]

Right to data portability

36. Data subjects will have the right to receive and transmit their personal data to other controllers when it has been previously provided in a commonly used and machine-readable format. This right applies where personal data that has been provided by an individual to a controller, the processing is based on consent or the performance of a contract; and processing is automated.[65]

Other rights enhancing measures

37. These data rights are enhanced by various other provisions. For example, the GDPR strengthens the conditions for consent, which must 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 their personal data, and can be withdrawn at any time.[66] The GDPR also provides that notification of a breach to the data subject will be mandatory where a data breach is likely to result in a "high risk to the rights and freedoms" of data subjects.[67]

The Data Protection Bill

38. At Second Reading, Lord Ashton of Hyde set out three objectives of the Bill. Firstly, that data must be secure with transparency over its use and a proportionate but rigorous enforcement regime. Secondly, the free flow of data across borders must continue to support trading relationships. Thirdly, to tackle crime and protect national security.[68] In sum, the Bill replaces the DPA; applies the GDPR; implements the UK's exemptions and derogations permitted by the GDPR; incorporates the EU Law Enforcement Directive; incorporates the Council of Europe's Convention for the Protection of

[63] Article 9(1) GDPR
[64] Articles 4(4), 9, 22 and Recitals 71 and 72 GDPR
[65] Articles 12, 20 and Recital 68 GDPR
[66] Article 4(1) and Recital 32, and Article 7(3) GDPR
[67] Article 34 GDPR. This is subject to caveats set out in Article 64(3).
[68] Lord Ashton of Hyde, Second Reading, Data Protection Bill [HL], 10 October 2017, Hansard Vol. 785, col.124

Individuals with Regards to the Automatic Processing of Personal Data; and sets up a data protection regime for the intelligence services.

IV. Human rights implications

i. Article 8 of the Charter on Fundamental Rights is not incorporated

39. Article 8 of the Charter, which has a central role in EU law on data protection and data processing, is not expressly incorporated into the Bill. Since the Charter gained EU treaty status in 2009, many decisions of the Court of Justice of the EU (CJEU) and the UK courts have relied on its provisions. A series of legal challenges to EU-third country and EU internal data protection instruments have demonstrated the importance of the Charter.[69] However, the Government proposes to exclude the Charter from "retained EU law" after exit day. Instead, underlying rights and principles will be retained.[70] It is unclear the extent to which the underlying rights and principles of Article 8 will be retained. The Department for Exiting the EU released its analysis of the Charter on 5 December 2017. This acknowledges that Article 8 of the Charter has no direct equivalent in the ECHR and refers to the Data Protection Bill as the means by which Article 8 (Charter) principles will be retained in domestic law after exit day.[71]

40. This raises a series of questions: how will retained EU data protection law be read so as to replace references to Article 8 of the Charter; will any aspects of the Charter right to data protection be lost because they are not reflected in enforceable law in the UK; and how are references in the GDPR to the Charter will be dealt with?[72] Arguably, implementing the GDPR will not be enough on its own to ensure a positive data adequacy finding for the UK if the Bill falls short of the standards required by Article 8 of the Charter.

41. Express inclusion of Article 8 of the Charter was discussed during Committee stage debate in the House of Lords. Lord Stevenson of Balmacara argued, *inter alia*, that given the exclusion of the Charter from retention in domestic law after exit day, the omission of Article 8 from the Bill is of even greater significance resulting in a totally unnecessary risk when the time comes for the EU to assess whether the UK's regime is equivalent to the rest of the

[69] In a recent opinion on an EU-Canada agreement on transferring personal data outside the EU, the Grand Chamber of the Court of Justice said that it would refer only to Charter Article 8 because that provision lays down the conditions of data processing in a more specific manner than Article 16 TFEU. See Opinion of the Court 1/15, Grand Chamber of the CJEU, 26 July 2017

[70] Clause 5(4) and (5) EU (Withdrawal) Bill

[71] Department for Exiting the EU, Charter of Fundamental Rights of the EU, Right by Right Analysis, 5 December 2017, p25-26

[72] The GDPR's Recitals refer to Article 8 and the substantive provisions refer to the Article 47 right to an effective remedy.

EU.[73] At Second Reading debate, Baroness Kidron stated, "we are told that this Bill is about data protection for individuals—a Bill that favours users over business and children over the bottom line. But the absence of Article 8 of the European Charter of Fundamental Rights is an inexcusable omission. The Bill in front of us is simply not robust enough to replace Article 8." [74] However, Lord Pannick suggested that giving "a special legal status to one charter right in isolation… is simply inappropriate".[75] He further explained that Article 8, like all the other rights in the European charter, is subject to the limitations stated in Article 52. The amendment, he argued, suggests Article 8 is absolute, which is "simply wrong".[76] The amendment to expressly include Article 8 was rejected.

42. **The Committee may wish to consider whether Article 8 of the Charter ought to be expressly included in the Bill (subject to the necessary limitations).**

ii. Conditions, Exemptions and Derogations

43. The data protection principles[77] and rights[78] set out in the GDPR are not absolute. A Member State may make exemptions to or derogate from them in pursuit of specified legitimate aims:
    a) Article 23(1) GDPR permits Member States to restrict the application of the data principles and rights provided that such restrictions respect the essence of fundamental rights and freedoms and are a necessary and proportionate measure in a democratic society to safeguard the prescribed aims which include, *inter alia*, national security; defence; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; other important objectives of general public interest; the protection of judicial independence and judicial proceedings; the protection of the data subject or the rights and freedoms of others; the enforcement of civil law claims.
    b) Article 23(2) provides that if the restriction meets the above criteria (in Article 23(1)), the legislative measure must contain specific provisions, where relevant, as to the purpose of processing; scope of the restrictions; safeguards to prevent abuse or unlawful access or

[73] Lord Stevenson of Balmacara, Committee debate [HL], 30 October 2017, Hansard, col. 1162-3
[74] Second Reading, 10 October 2017, Hansard, col.187-9
[75] Lord Pannick, Committee debate [HL], 30 October 2017, Hansard, vol. 785 col. 1166
[76] *Ibid.*
[77] Article 5, GDPR
[78] Article 12 – 21 GDPR

transfer; storage periods; and risks to the rights and freedoms of data subjects.[79]

c) Article 85(2) allows Member States to reconcile data protection rights with the right to freedom of expression and information, including data processing for the purpose of journalism; academic expression; literary expression; and artistic expression.[80]

44. In accordance with Article 23(1) and 85(1) of the GDPR, Part 2 of the Bill sets out the UK's exemptions and derogations to the data protection principles and rights. The Bill provides for such restrictions on the numerous grounds, including: national security;[81] prevention or detection of crime;[82] apprehension or prosecution of offenders;[83] maintenance of effective immigration control;[84] disclosures required by law or in connection with legal proceedings;[85] functions designed to protect the public; various regulatory services relating to law, health, and children;[86] parliamentary privilege; judicial appointments, judicial independence, and judicial proceedings; conferring honours, dignities, and appointments; protection of the rights of others; journalistic, academic, artistic or literary purposes;[87] research, statistics, and archiving;[88] health, social work, education, and child abuse data;[89] disclosure prohibited or restricted by an enactment.[90]

45. The Government asserts that any interference with rights is necessary, proportionate and in pursuit of a legitimate aim.[91] Whilst the above grounds may reasonably require exemptions or derogations from *some* data protection principles or rights, the breadth of the exemptions from even the most fundamental rights and principles requires scrutiny. A few of the exemptions are of particular concern given their interference with the right to privacy and data protection:

a) the exemptions permitted on the grounds of "effective immigration control";

b) the exemptions from the right not to be subject to automated decision-making;

[79] A full list of the specific provisions required is set out in Article 23(2) GDPR.
[80] Article 85(1) GDPR
[81] Clause 24 of the Bill
[82] Schedule 2, Part 1, paragraph 2(1)(a) of the Bill
[83] Schedule 2, Part 1, paragraph 2(1)(b) of the Bill
[84] Schedule 2, Part 1, paragraph 4(1)(a) of the Bill
[85] Schedule 2, Part 1, paragraph 5 of the Bill
[86] Schedule 2, Part 2, paragraph 8 and 9 of the Bill
[87] Schedule 2, Part 5, paragraph 24 of the Bill
[88] Schedule 2, Part 6, paragraph 25 – 26 of the Bill
[89] Schedule 3 of the Bill
[90] Schedule 4 of the Bill
[91] Explanatory Notes to the Bill, para 808

c) the exemptions from the prohibition of processing special categories of data;[92]
d) the exemptions permitting cross-border transfers in the public interest;
e) the exemptions permitted by national security certificates;[93]
f) the exemptions permitted for the intelligence services; and
g) the exemptions permitted for the purpose of freedom of expression.

a. Immigration control

46. The GDPR does not expressly provide for immigration control as a legitimate ground for exemption. However, the Bill creates an exemption from certain provisions of the GDPR for the "maintenance of effective immigration control" or "the investigation or detection of activities that would undermine the maintenance of effective immigration control."[94] The Minister for State described this exemption as "a necessary and proportionate measure to protect the integrity of our immigration system."[95]

47. When processing data on immigration grounds, exemptions are applied to almost every data protection right and every data protection principle.[96] This exemption not only interferes with Article 8 rights but also Article 10, as it removes the individual's right of access to information. In written evidence, Open Rights Group submits that subject access requests are an integral part of many immigration cases.[97]

48. Concerns have been raised in the House of Lords that this exemption is wide-ranging and may be open to abuse.[98] This exemption would not only apply to the Home Office, but to any entity that shares data with the Home Office for immigration control purposes. Liberty notes that data-sharing agreements between the Home Office and frontline agencies are often concluded in secret and subject to negligible parliamentary scrutiny,[99] warning that "effective immigration control is a highly subjective goal, with the parameters and the effects on individuals' human rights vulnerable to political tides".[100] The Equality and Human Rights Commission submits that this exemption could "permit the authorities to access and process highly personalised data, for

[92] Clause 9 of the Bill: 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.
[93] Clauses 24, 41(4), 42(4), 45(3), 65(7), and 110 of the Bill
[94] Schedule 2, Part 1, paragraph 4 of the Bill
[95] Baroness Williams, Committee debate [HL], 13 November 2017, Hansard vol.785 col.1913
[96] Exemptions are permitted to the right to information; right of access; right to rectification; right to erasure; right to restriction of processing; right to data portability; right to object; and all the principles in Article 5 GDPR. See Schedule 2, Part 1, para 1 of the Bill.
[97] Open Rights Group, Written Evidence, DPB0005, November 2017, p3
[98] Lord Clement-Jones, Committee debate [HL], 13 November 2017, Hansard, vol. 785, col. 1909
[99] Liberty, Written Evidence, DPB0002, November 2017, p12
[100] *Ibid*., p10

example, phone or social media data relating to sexual lives of immigrants claiming residency rights on the basis of their relationship with a British citizen."[101]

49. This exemption would seem to apply to all individuals engaged in the immigration system, including EU citizens, as well as British citizens who are spouses or family members of those engaged in the immigration system. Naturally, this exemption may apply to nationals and non-nationals, but is likely to have a greater impact on non-nationals. Any discrimination on the basis of nationality would engage Article 14 (in conjunction with Article 8 ECHR), as well as Articles 7, 8 and 21 of the Charter.

50. The immigration exemption represents a departure from the current regime under the DPA. It is not clear why this exemption is "necessary in a democratic society". Firstly, the Bill provides for exemptions in relation to the investigation and detection of crime,[102] which could be applied in the context of illegal immigration in some instances. Secondly, even where the crime exemption would not apply, it is unclear why immigration control requires exemptions from fundamental principles such as lawfulness, fairness, and accuracy in order to maintain its effectiveness. Baroness Williams of Trafford gave two examples during Committee debate in order to justify this exemption; the first scenario was that of a "suspected over-stayer" and the second was of someone providing false information in an application for leave to remain.[103] Even in these scenarios, it is not clear why such basic principles should be extinguished. It is arguably disproportionate to extend such restrictions to immigration control, particularly so in relation to lawful immigration.

51. Article 23(1) of the GDPR states that an exemption made under this Article must respect "the essence of the fundamental rights and freedoms" and must be "a necessary and proportionate measure in a democratic society". Further, Article 23(2) states that any exemptions must set out the scope of the restrictions introduced; the safeguards to prevent abuse or unlawful access or transfer; and the risks to the rights and freedoms of data subjects. The immigration exemption appears to fall foul of the safeguards required by Article 23. In written evidence to the Committee, a number of organisations raised concerns regarding this exemption. Privacy International and Open Rights Group submit that it represents a dramatic departure from

[101] The Equality and Human Rights Commission, Written Evidence, DPB0006, November 2017, p4
[102] Article 23 GDPR permits Member States to make exemptions to data rights on the grounds of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.
[103] Baroness Williams of Trafford, Committee debate [HL], 13 November 2017, Hansard vol. 785, col. 1914. Further explanation is given in a letter from Baroness Williams of Trafford to Lord Clement-Jones, dated 23 November 2017, published with the Bill documents on gov.uk

proportionate restrictions on fundamental rights and calls for its removal from the Bill.[104] Amnesty International submits that the immigration exemption would significantly increase the risk that people, including British citizens, are harmed.[105] They point to the fact that the data controller (most likely the Home Office) would be responsible for determining whether the data protection safeguards would be "likely to prejudice" effective immigration control. The body against whom the safeguards apply would therefore determine whether or not to exempt itself from these safeguards.[106] An amendment was tabled in the House of Lords to remove this exemption from the Bill, but was withdrawn.[107]

52. **The Committee may wish to consider whether an exemption for effective immigration control is necessary and proportionate given the broad reach this exemption would have. The Committee may wish to make further enquiries of the Government as to the justification for this exemption.**

b. Automated decision-making and profiling

53. The Government states that the Bill will give individuals greater say in decisions that are made about them based on automated processing.[108] Strict safeguards are required where personal data is processed for automated decision-making or profiling without human input, given the impact such decisions can have on individuals. Individuals have a qualified right not to be subject to automated decision-making. Where exceptions apply such that automated decision-making and profiling is permitted, individuals have a right to access information relating to automated decisions that affect them. Where decisions are based solely on automated processing, individuals can request that processing is reviewed by a person rather than a machine.[109]

54. In written evidence, Privacy International submits that "reliance on algorithms and machine learning may pose a number of challenges, including with regards to opacity and auditability of the processing of data as well as accountability for decisions which impact individuals' human rights."[110] They further submit that inferred profiles may be inaccurate or systematically biased, and may lead to individuals being misclassified in a way that may result in harm and the enjoyment of their rights.[111] For example, in racially

[104] *Ibid*., p2, Privacy International, Written Evidence, para 4.8.1
[105] Amnesty International, Written Evidence, DPB0001, November 2017, para 21
[106] Ibid., para 14
[107] Amendment 80: Schedule 2, page 125, line 41, leave out paragraph 4
[108] Department of Culture, Media and Sport, Statement of Intent ,p8-9
[109] Article 22 GDPR, Clause 13 of the Bill
[110] Privacy International, Written Evidence, DPB0004, November 2017, p24, para 5.6.6
[111] *Ibid*., p25, para 5.6.9

segregated cities, postcodes may be a proxy for race - profiling using postcodes may lead to a discriminatory outcome.[112] As noted by the U.N. Human Rights Council, "automated processing of personal data for individual profiling may lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights, including economic, social and cultural rights."[113]

55. The Bill provides a right to object to automated decision-making where a decision based *solely* on automated processing has legal effects or similarly significant effects.[114] This precludes individuals from objecting to automated decision-making with minimal human input. There may be decisions taken with minimal human input that remain *de facto* determined by an automated process that have significant consequences for the individual, including consequences for their rights. Liberty raised particular concerns about the application of this exemption to law enforcement processing, citing algorithms currently being trialed by police forces such as the harm assessment risk tool used in bail decisions and the automated facial recognition software that supports officers decisions and leads to arrests.[115] Arguably, decisions that are *de facto* automated ought to be subject to the right to object.[116]

56. As such, protection should be extended beyond *solely* automated decisions. Individuals must have the right to an explanation and the right to challenge *de facto* automated decisions.[117] Both Privacy International and Liberty support amendments to prohibit automated decisions that affect human rights.[118] Amendments of this nature were tabled at Committee stage, but were dismissed by Ministers as "wholly negat[ing] the provisions in respect of automated decision-making."[119]

57. **The Committee may wish to consider whether automated decision-making requires further safeguards and more specifically whether automated decisions significantly affecting human rights should be restricted or prohibited.**

c. Special categories of personal data

[112] *Ibid*., p25, para 5.6.9
[113] UNHRC Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRD/34/7, 23 March 2017, para 2, Privacy International, Written Evidence, November 2017, p23
[114] For general automated processing – clause 13; for law enforcement automated processing – clause 47; for intelligence services automated processing – clause 94
[115] Liberty, Written Evidence, November 2017, p15
[116] Privacy International, Written Evidence, November 2017, p24-26
[117] Privacy International, Written Evidence and Liberty, Written Evidence, November 2017
[118] Privacy International, Written Evidence, November 2017, para 5.11.1, p30
[119] Lord Ashton of Hyde, Committee stage, HL, 13 November 2017, Hansard vol.785 col. 1871

58. The GDPR prohibits the processing of special categories of personal data, with some exceptions.[120] Where personal data falls into these sensitive categories, conditions must be met. The Bill exempts the following categories from the ban on processing special categories of data:[121]
    a) Employment, social security and social protection;
    b) Substantial public interest;
    c) Health and social care;
    d) Public health;
    e) Archiving, research and statistics;
    f) Criminal convictions data.[122]

59. These exemptions are subject to the conditions and associated safeguards laid out in Schedule 1.[123] In particular, processing of special category data and criminal convictions data should only be carried out if safeguards for the fundamental rights of the data subject are provided for.[124] The data controller must also have an appropriate policy in place and must keep this under review.[125] The Government considers that where any such exemptions interfere with Article 8, the interference is necessary, proportionate, and in pursuit of a legitimate aim.[126]

60. However, the Bill fails to clearly define terms. Firstly, the term "fundamental rights" is undefined. It is unclear which data rights and which non-data rights might fall within this definition. Secondly, the terms "substantial public interest" and "public interest" are undefined.[127] Under the Bill as currently drafted, the Information Commissioner's Office (ICO) has discretion as to the publication of guidance on the "public interest" test.[128] In written evidence, Privacy International submits that clarification of these terms is required and guidance from the ICO should be mandatory to prevent misapplication of these terms leading to arbitrary interferences with individuals' rights.[129]

61. Amongst the "substantial public interest"[130] conditions is an exemption which permits political parties to process personal data revealing political opinions

[120] Article 9(1) and 9(2) GDPR
[121] Clause 9(1) of the Bill
[122] Clause 9 of the Bill. Clause 9(5) provides for the processing of criminal convictions data (as permitted by Article 10 of the GDPR) – separate to the special categories of data.
[123] Note that the Secretary of State is given a broad power to make regulations to amend Schedule 1 by adding, varying, or omitting conditions or safeguards (discussed below).
[124] Article 9(2)(g) GDPR
[125] Explanatory Notes, paras 577-578
[126] Explanatory Notes, para 810
[127] Clause 7 of the Bill. See Article 6(1) GDPR – processing shall be lawful only if one of the following applies…. (e) necessary for a task carried out in the public interest.
[128] Privacy International, Written Evidence, DPB0004, November 2017, para 4.6.8
[129] *Ibid*., para 4.6.7
[130] Schedule 1, Part 1 to the Bill

for the purpose of political activities.[131] Privacy International has expressed particular concern with this condition, which goes beyond the GDPR, and considers that it does not appear necessary for electoral activities in a democratic system:[132]

> "Whilst we appreciate that a variation of this condition was included in Schedule 3 to the DPA, technology and data processing in the political arena has moved on. The processing of personal data plays a key part in political activities (including political parties contracting the services of specialist data mining companies), and this is only likely to increase going forward. Personal data that might not have previously revealed political opinions can now be used to infer information about the political opinions of an individual (primarily through profiling). We do not consider that this condition meets the requirements of Article 9(2) of GDPR, it is not demonstrably in the substantial public interest and it is not proportionate."[133]

62. **The Committee may wish to consider whether the Bill provides sufficient clarity as to the meaning of "substantial public interest" and "public interest" and whether the safeguards for processing special categories data are sufficient.**

d. Cross-border transfers in the public interest

General data transfers

63. The GDPR allows Member States to make provision for the international transfer of personal data.[134] In relation to general data processing, clause 17 enables the Secretary of State, in the absence of an adequacy decision or safeguards, to make regulations specifying the circumstances that would allow for the transfer of data to a third country[135] or international organisation where necessary for important reasons of public interest.[136] It also allows the Secretary of State to specify limitations on such data transfers.[137] The European Commission decides whether third countries or international organisations offer an adequate level of data protection providing legal certainty and uniformity for the EU. Where the Commission has not recognised a third country or international organisation as adequate, cross-border transfers may only occur in accordance with the provisions of the Bill.

64. If the Secretary of State were to exercise this power under clause 17, personal data could be transferred outside the UK without an adequacy decision or appropriate safeguards if the Minister considered it to be in the

[131] Schedule 1, Part 2, para 18 to the Bill
[132] Privacy International, Written Evidence, DBP0004, November 2017, p19
[133] Privacy International, Briefing on the Data Protection Bill for Second Reading, 6 October 2017, p.7
[134] Article 49(4) and (5) GDPR
[135] I.e. not a member of the EU or EEA
[136] Clause 17 of the Bill
[137] Clause 17(2) of the Bill

"public interest".[138] This is problematic given the lack of definition of "public interest". Although the Government points out that such regulations would be subject to parliamentary scrutiny[139], as currently drafted would only be subject to the negative procedure.

Law enforcement data transfers

65. The Bill also provides for law enforcement agencies to make cross-border transfers, in the absence of an adequacy decision, for law enforcement purposes if certain conditions are met and the transfer is authorised by a competent authority.[140] Where there is no adequacy decision, cross-border transfers must be necessary for the purpose of law enforcement and either based on appropriate safeguards or special circumstances.[141] Appropriate safeguards must either be contained in a legally binding instrument, or the data controller must determine that appropriate safeguards are in place based on an assessment of all the circumstances (e.g. agreements with Europol and Eurojust).[142] These conditions do not apply where the data transfer is necessary for the prevention of an immediate and serious threat to the public security of a Member State or a third country or the essential interests of a Member State, and authorisation cannot be obtained in good time.[143]

66. Where there are no appropriate safeguards in place, the transfer may still be made if any of the following "special circumstances" exist:
    a) to protect the vital interests of the data subject or another person;
    b) to safeguard the legitimate interests of the data subject;
    c) for the prevention of an immediate and serious threat to the public security of a member State or a third country;
    d) in individual cases for any of the law enforcement purposes; or
    e) in individual cases for a legal purpose.[144]

67. However, (d) and (e) do not apply if the "fundamental rights and freedoms" of the individual override the "public interest".

Intelligence services data transfers

68. Intelligence agencies may make cross-border transfers, where necessary and proportionate, in accordance with their statutory functions or provisions of the *Security Services Act 1989* or *Intelligence Services Act 1994* (i.e. in the interests of national security, the prevention or detection of serious crime, or for the purpose of criminal proceedings). There are no requirements on the

[138] Undefined but a non-exhaustive list of examples is provided in clause 7.
[139] Explanatory Notes, para 813
[140] Clause 71(1) of the Bill
[141] Clause 71 (3) of the Bill
[142] Clause 73 of the Bill
[143] Clause 71(5) of the Bill
[144] Clause 74 of the Bill

intelligence services to ensure appropriate safeguards are in place or that special circumstances exist.

69. Beyond the Bill, Privacy International submits that the domestic legal framework governing intelligence sharing fails to provide any additional safeguards. In particular, they note that the clandestine nature of intelligence-sharing agreements between agencies across jurisdictions means that they are not subject to any oversight or public scrutiny.[145] The Independent Reviewer of Terrorism Legislation has noted that there is "no statute or Code of Practice governing how exchanges [to foreign authorities] should be authorised or take place".[146]

70. In the absence of constraints in other statutes, the Bill provides the intelligence agencies with unfettered powers to transfer personal data across borders without any appropriate levels of protection in place or any regard for the protection of individuals' rights. The Government states that the Bill is consistent with EU Convention 108,[147] which permits states to derogate from rights in the interests of state security.[148] However, such derogations are only permitted where "necessary in a democratic society". The European Court of Human Rights has held that, "since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power."[149]

71. **The Committee may wish to consider whether the powers contained within the Bill permitting cross-border transfers are necessary and proportionate. The Committee may want to pay particular attention to the unfettered powers granted to the intelligence services in the absence of any safeguards. The Committee may also wish to engage with the Intelligence and Security Committee and the Independent Reviewer of Terrorism Legislation to explore these matters further.**

e. National security and defence exemptions

72. National security certificates may be issued by the Secretary of State which provide exemptions from data rights and principles. The Government states that national security falls outside of the scope of EU law and therefore outside of the GDPR.[150] As such, any processing of personal data related to

[145] Privacy International, Written Evidence, DPB0004, November 2017, p58-60
[146] D. Anderson, 'A Question of Trust: Report on the Investigatory Powers review', June 2015, para 7.66. PI evidence, p60, para 7.13
[147] Explanatory Notes, para 816
[148] Article 9, Convention 108
[149] *Weber and Saravia v Germany,* (2008) 46 EHRR SE5, para 93
[150] Explanatory Notes, para 122

national security will be governed by the "applied GDPR".[151] Whilst Article 4(2) of the Treaty on European Union provides that "national security remains the sole responsibility of each Member State", despite this, EU data protection legislation provides for derogations for national security.[152] If national security was entirely outside the scope of EU treaties, such derogations would be unnecessary. Arguably, these provisions imply the retention of some level of EU scrutiny over derogations from EU data protection rights on the grounds of national security.

73. Clauses 24-26 create exemptions from certain provisions of the "applied GDPR" for the purpose of safeguarding "national security" or for "defence purposes".[153] Neither "national security" nor "defence purposes" are defined within the Bill or the Explanatory Notes. A Minister's certificate is "conclusive evidence of [the] fact" that the exemption is required for national security or defence purposes.[154] It is not clear which organisations will be the beneficiaries of these certificates. Where either "national security" or "defence purposes" are relied upon, exemptions apply to nearly all the data protection principles,[155] all the rights of data subjects,[156] certain obligations on data controllers and processors,[157] and various enforcement provisions.[158] National security certificates are indefinite - the Bill does not impose a time limit or a duty to review the ongoing necessity of the certificate.

74. Similar national security exemptions are provided for law enforcement data processing[159] and data processing by intelligence agencies.[160] However, the intelligence services are granted even more extensive exemptions, including exemptions from the oversight of the Information Commissioner.[161] The effect of these exemptions is to allow Ministerial certificates to override the powers of the Information Commissioner.

75. There are some examples which clearly demonstrate why certain exemptions are required. For example, an intelligence agency data controller will require an exemption from having to notify a terrorist suspect subject to surveillance

[151] Chapter 3 Part 2 of the Bill. The applied GDPR applies relevant Articles of the GDPR to general data processing outside the scope of EU law (set out in Schedule 6). After the UK's withdrawal from the UK, there will no longer be a distinction.
[152] For example, the existing Data Protection Directive (DPD) (Article 13), the new GDPR (Article 23) and the existing E-Privacy Directive (Article 15 (1)).
[153] Clauses 24, 41(4), 42(4), 45(3), 65(7), and 110 of the Bill
[154] Clause 25 of the Bill
[155] Clause 24(2)(a) of the Bill
[156] Clause 24(2)(b) of the Bill
[157] Clause 24(2)(c) and (d) of the Bill
[158] Explanatory Notes, para 161
[159] Clause 77
[160] Clauses 108-109
[161] Clause 108 exempts intelligence services from provisions in Schedule 13 concerning the functions of the Information Commissioner: paragraphs 1(a), 1(g) and (2).

that his/her data is being processed.[162] However, it is unclear why the authorities require such a breadth of exemptions from their obligations under the data protection regime. Some of the data protection principles ought arguably to apply to even where national security or defence exemptions apply. For example, why do the authorities require an exemption from the principle that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes?[163]

76. The Government states that the national security exemptions in the Bill mirror the current situation under the DPA and do not, therefore, constitute a greater interference with rights than at present.[164] Maintenance of the *status quo* is not a sufficient justification with such a broad power to interfere with privacy rights. The Committee may wish to bear in mind that in order for an interference with rights to be "in accordance with law", it must include safeguards against arbitrary interference. The provisions regarding national security certificates arguably fall short of this requirement.

77. **The Committee may wish to consider whether the broad and indefinite exemptions granted by national security certificates are a necessary and proportionate interference with the data protection principles and rights of data subjects. The Committee may also wish to consider recommending the strengthening of oversight for the issuing of national security certificates. The Committee may also wish to engage with the Intelligence and Security Committee and the Independent Reviewer of Terrorism Legislation to explore these matters further.**

78. A data subject may appeal against the issuing of a national security certificate, but this is limited to judicial review rather than a challenge on the merits. This reflects the current regime under the DPA.[165] Under section 28 of the DPA, where an individual requests to access his/her data which is subject to a certificate, the individual will merely be informed that they have been given all the information that is required under the Act (an "NCND" response). The individual would not be informed that their data is being withheld on the grounds of a national security certificate. This problematic situation would be replicated under the Bill. This makes it difficult for an individual to appeal a certificate because any person "directly affected" by a certificate would not be notified of this fact. It is unclear how the right to judicial review could be

[162] Explanatory Notes, para 271
[163] The second data protection principle, clause 85(1) of the Bill
[164] Explanatory Notes, para 815
[165] Section 28 DPA`1998

exercised without any way of knowing whether a national security certificate has been applied to their data.[166]

79. Further, a tribunal may only quash a certificate if the Minister did not have reasonable grounds for issuing the certificate. It is not clear whether wider grounds of judicial review apply. In any event, the tribunal would be precluded for considering the merits of the decision. The appeal rights of individuals are therefore restricted to a costly and narrow avenue of appeal.[167]

80. Privacy International submits that some national security certificates that have been disclosed as a result of legal proceedings have been quashed as unlawful.[168] However, there is no requirement for such certificates to be made public and in general they will not be disclosed outside of legal proceedings. In Committee stage debate, the Minister of State, Baroness Williams of Trafford, argued that national security certificates are "public in nature". She further stated her commitment to making certificates "more accessible in the future".[169] Given the clandestine nature of national security certificates, there is a risk that such certificates may be unnecessary and/or disproportionate and entirely devoid of scrutiny. The lack of transparency may also be a barrier to effective judicial remedies for individuals to enforce their rights.

81. **The Committee may wish to consider whether the national security exemption is a proportionate interference with the rights of data subjects and further whether the right of appeal provides an effective judicial remedy.**

f. Intelligence services

82. The Bill provides for a 'bespoke' data processing regime for the intelligence agencies that provides for exemptions for a wide range of principles and rights, as well as reduced safeguards compared to the general and law enforcement data processing regimes. Given the broad exemptions applicable to intelligence services, there are a number of concerns as to whether the interferences with individual rights are in accordance with the law, necessary and proportionate.

83. Firstly, the intelligence services are permitted to process personal data, *inter alia*, in the interests of the controller or the third party to whom the data is

[166] Privacy International, Briefing on the Data Protection Bill for Second Reading, 6 October 2017
[167] This draws upon a similar debate that was had regarding the oversight regime provided for in the Investigatory Powers Act 2016 (i.e. the powers given to Judicial Commissioners to review executive decisions under the IPA were also limited to judicial review principles, as opposed to powers to review the merits of executive decisions).
[168] *Norman Baker MP v SSHD* [2001] UKHRR 1275 and Privacy International, Written Evidence, DPB0004, November 2017
[169] Privacy International, Written Evidence, DPB0004, November 2017, para 6.54, p44

disclosed.[170] This 'legitimate interest' condition does not apply to other public authorities and is arguably too broad and opaque.[171]

84. Secondly, Schedule 11 sets out the rights, principles and obligations from which intelligence services are exempt when processing data for certain purposes, such as the prevention or detection of crime[172] or economic well-being of the UK.[173] When an exemption applies, all of the data protection rights and nearly all of the data protection principles are disapplied. As discussed above, national security certificates nullify nearly all the data protection principles, including the eighth principle, that "personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."[174] Further, intelligence services are exempted from the right of data subjects to apply to court for an order against a data controller or processor for violating their data protection rights.[175]

85. Thirdly, the obligations imposed upon intelligence agencies in relation to personal data breaches are less stringent than those imposed upon law enforcement agencies. For example, law enforcement agencies are required to inform data subjects of a breach where the breach is "likely to result in high risk to the rights and freedoms of individuals" (with some exceptions).[176] Conversely, intelligence agencies are only required to report "serious" personal data breaches to the Commissioner. A breach is "serious" if it "seriously interferes with the rights and freedoms of a data subject".[177] Any data breaches that the intelligence agencies consider less than serious will go unreported.

86. There is clear no justification for such broad exemptions to apply to the intelligence services, nor any reason why such exemptions should preclude fundamental rights and principles such as the requirement that data processing must be for a specified, explicit and legitimate purpose[178] and personal data must be kept for no longer than is necessary for the purpose for which it is processed.[179]

[170] Schedule 9, para 6, to the Bill
[171] Schedule 1, para 6, to the Bill
[172] Schedule 11, para 2, to the Bill
[173] Schedule 11, para 1, to the Bill
[174] Clause 24(2)(a) of the Bill
[175] Clause 158(4)(b) of the Bill
[176] Clause 66(1) of the Bill
[177] Clause 106(7) of the Bill
[178] Second data protection principle, clause 85(1), Chapter 2, Part 4 of the Bill
[179] Fifth data protection principle, clause 88 of the Bill

87. **The Committee may wish to consider whether the significantly reduced safeguards for intelligence services are necessary and proportionate and whether there is sufficient oversight given the broad and unfettered powers.**

g. Freedom of expression and information

88. There is often an inherent tension between Article 8 and Article 10 ECHR. Both Articles are qualified and can be justifiably interfered with by the other. Article 85 of the GDPR requires Member States to provide exemptions or derogations in the context of processing personal data for the following "special purposes":
    a) journalism;
    b) academic, artistic or literary expression; or
    c) if necessary to reconcile the right to protection of personal data with the right to freedom of expression.

89. The Bill provides for a broad exemption for data processing for the above purposes. Publications of personal data for the above special purposes must be reasonably considered to be in the public interest, taking account of the special importance of the public interest in freedom of expression and information and relevant codes of practice.[180] In particular, the exemptions for "special purposes" apply to the extent that the processing must be undertaken with "a view to" publication; the data controller reasonably believes that publication would be in the public interest; and the data controller reasonably believes that in all the circumstances compliance is incompatible with the special purpose.[181] However, concerns have been raised within the media regarding the Information Commissioner's powers to determine whether these conditions have been met. It has been argued that this is an inappropriate power and may infringe the freedom of expression of journalists.[182]

90. In order to allow for the publication of such material, Part 4 of Schedule 2 to the Bill provides exemptions from the data protection principles, many of the rights of data subjects, and some of the obligations upon controllers. However, the 'freedom of expression' exemptions have been the subject of some concern. At Second Reading, Baroness Hollins highlighted numerous examples of data abuses committed by journalists and stated that "the Bill in its current form does not provide an adequate balance between privacy and freedom of expression… Freedom of expression is essential to hold power to account and to expose wrongdoing, and it must be protected. However, the

[180] Schedule 2, Part 5, paragraph 24, to the Bill
[181] Schedule 2, Part 5, paragraph 24(2), to the Bill. This reflects section 32 of the DPA 1998
[182] Commissioner's powers set out in clause 164(3). See for example, R. Greenslade, The Guardian, 'The data protection bill is yet another legal threat to UK press freedom', 3 December 2017.

public also need to be protected from those who might seek to abuse such freedoms with the primary business purpose of selling newspapers."[183] Concerned with the "blank cheque", Baroness Hollins argued that the exemption would allow journalists to breach data rights with little protection for the public from abuse.[184]

91. **The Committee may wish to consider whether the Bill strikes the right balance between the right to privacy and protection of personal data and the right to freedom of expression and information.**

iii. Delegated powers

92. There are a number of clauses within the Bill that give Ministers the power to make regulations that may interfere with the right to privacy and data protection without the checks and balances afforded to primary legislation. In particular, Ministers are given powers to create new exemptions to data protection rules[185] as well as adding or removing exemptions to the safeguards for processing of "special categories of data".[186] These powers have been criticised by both the Delegated Powers and Regulatory Reform Committee and the House of Lords Constitution Committee.[187]

93. Schedule 1 of the Bill provides numerous exemptions to the general prohibition on the processing of "special categories of data".[188] Clause 9(6) permits the Secretary of State to make regulations amending Schedule 1 by adding, varying, or omitting the conditions or safeguards. Noting that these powers would allow for the most sensitive types of personal data to be processed in entirely new circumstances, the Delegated Powers and Regulatory Reform Committee stated that "it is inappropriate for Ministers to be given carte blanche to rewrite any or all of the conditions and safeguards in Schedule 1 by regulations in order to 'deal with changing circumstances' instead of bringing forth a Bill."[189]

94. Schedules 2, 3, and 4 of the Bill set out a large number of exemptions to data rights and principles. Clause 15 provides a delegated power for the Secretary of State to amend the exemptions to the data protection principles and rights beyond those provided for by the GDPR, allowing the Secretary of State to

[183] Baroness Hollins, Committee debate [HL], 6 November 2017, Hansard vol. 785, col.1661
[184] *Ibid*
[185] Clauses 15 and 111 of the Bill
[186] Clauses 9, 33, and 84 of the Bill
[187] Delegated Powers and Regulatory Reform Committee Sixth Report 6th Report of Session 2017-19, 24 October 2017, HL Paper 29; House of Lords Constitution Committee, Data Protection Bill, Sixth Report of Session 2017-19, HL Paper 31, p4, para 11
[188] Schedule 1 of the Bill
[189] Delegated Powers and Regulatory Reform Committee Sixth Report 6th Report of Session 2017-19, 24 October 2017, HL Paper 29, para 20

create new legal bases for the performance of tasks in the public interest or in the exercise of public authority. Although this is subject to the affirmative procedure, this is a broad power allowing the Secretary of State to alter the rights of data subjects. The Delegated Powers Committee considers that the affirmative procedure "is not an adequate substitute for a Bill allowing Parliament fully to scrutinise proposed new exemptions to data obligations and rights."[190]

95. Schedule 8 of the Bill sets out the exemptions (or 'conditions') to the prohibition on special categories of data processing by law enforcement.[191] Clause 33(6) provides the Secretary of State with powers to add, vary or omit these conditions. Similarly, Schedule 10 limits the basis on which the intelligence services can process special categories of data. Clause 84(3) gives the Secretary of State the power to amend these conditions. Finally, Schedule 11 exempts the intelligence services from various obligations within the Bill. Clause 111 gives the Secretary of State the power to add to, amend, or repeal the exemptions prescribed by Schedule 11. As noted by the Delegated Powers Committee, although the Delegated Powers Memorandum states that this power will be used "if the Secretary of State considers that the exemption is necessary for safeguarding the interests of data subjects or the rights and freedoms of others", the Bill does not contain any such limitation on when the power can be used.[192]

96. Privacy International submits that conditions for processing of personal data (especially special categories of personal data) and any exemptions to the rights and obligations under the Bill (and GDPR) should be clearly set out on the face of the Bill.[193] MedConfidential submits that any permanent exceptions to data protection law must only be done via transparent democratic approval of Parliament through primary legislation, and expressed particular concern with the Government's "obsession with immigrant hunting" and complete disregard for privacy of patient data held by the NHS.[194]

97. Given the wide-ranging nature of the powers granted to Ministers, the Bill creates an uncertainty for individuals as to the future security of their rights. Liberty submits that the regulation-making powers must be removed, narrowed or, at a minimum, there must be a consultation and assessment of

[190] *Ibid.,* para 34
[191] At paragraphs 1 – 6: to protect the data subject's vital interests; where the personal data is already in the public domain; judicial and statutory purposes; legal claims and judicial acts; preventing fraud; archiving; research and statistical purposes.
[192] Delegated Powers and Regulatory Reform Committee Sixth Report 6th Report of Session 2017-19, 24 October 2017, HL Paper 29, para 33
[193] Privacy International, Written Evidence, DBP0004, November 2017, para 2.2
[194] MedConfidential Written Evidence, DBP0003, November 2017,, p1, para 5 and p2 para 10

the impacts on the rights of individuals.[195] Following deep concern in the House of Lords, Baroness Williams stated that the Government is "carefully considering the Delegated Powers Committee's report and will respond before the next stage of the Bill."[196]

98. **Following the Government's reconsideration of these provisions, t**he **Committee may wish to consider the necessity and proportionality of any delegated powers that are retained at Report stage, in light of the breadth of the powers and the potential to remove rights without Parliamentary scrutiny.**

iv. The right to a fair trial

99. A number of provisions in the Bill engage Article 6 ECHR, including:
    a) various defences to data offences that reverse the burden of proof, putting the onus on the defendant to "prove" his/her defence;[197]
    b) national security certificates issued by the Secretary of State that may only be appealed on judicial review principles; and
    c) civil society organisations which are prohibited from bringing a challenge under the Bill unless they are instructed by a litigant.

a. Reverse Burdens

Legal principles

100. Article 6(2) ECHR provides that everyone charged with a criminal offence shall be presumed innocent until proven guilty according to law. Reverse burden provisions that require the defendant to prove certain elements of his or her defence do not necessarily violate Article 6(2) as long as the overall burden remains with the prosecution[198] and any presumptions of law or fact against a defendant are within reasonable limits.[199]

101. In *Sheldrake v DPP*, the leading case on reverse burdens, Lord Bingham of Cornhill analysed both domestic and Strasbourg authorities and summarized:

> "The Convention does not outlaw presumptions of fact or law but requires that these should be kept within reasonable limits and should not be arbitrary. It is open to states to define the constituent elements of a criminal offence, excluding the requirements of *mens rea*. But the substance and effect of any presumption adverse to a defendant must be examined, and must be reasonable. Relevant to any

[195] Privacy International, Briefing on the Data Protection Bill for Second Reading, 6 October 2017, p.7, para 2.5
[196] Baroness Williams, Committee Stage [HL], 15 November 2017, Hansard vol. 785, col. 2063
[197] Clauses 139, 160, 163, and 171 of the Bill
[198] *Lingens v Austria* (1982) 4 EHRR 373
[199] *Salabiaku v France* (1988) 13 EHRR 379; *R v G* [2008] UKHL 37, [2009] 1 AC 92

> judgment on reasonableness or proportionality will be the opportunity given to the defendant to rebut the presumption, maintenance of the rights of the defence, flexibility in application of the presumption, retention by the court of a power to assess evidence, the importance of what is at stake and the difficulty which a prosecutor may face in the absence of a presumption. Security concerns do not absolve member states from their duty to observe basic standards of fairness. The justifiability of any infringement of the presumption of innocence cannot be resolved by any rule of thumb, but on examination of all the facts and circumstances of the particular provision as applied in the particular case."[200]

102. In *R v Roy Clarke*, the Court of Appeal took into account the following questions when considering whether a reverse legal burden was compatible with Article 6(2):

a) What does the prosecution have to prove in order to transfer the burden to the defendant?
b) Does the burden imposed on the accused relate to something which is likely to be difficult for him to prove, or does it relate to something which is likely to be within his knowledge or to which he has ready access?
c) What is the nature of the threat to society which the provision is designed to combat?[201]
d) What is the seriousness of the penalty faced by the accused?[202]

103. In this case, the court made "every allowance for the vital importance of ensuring that both factual and legal presumptions [were] kept within reasonable limits and not arbitrarily imposed or lacking in proportion",[203] and held that the imposition of a legal burden on the defendant to establish himself as a qualified immigration practitioner was both justified and proportionate. In so finding, the Court gave the following reasons: firstly, in order to transfer the onus to a defendant in cases such as these, the prosecution must first establish, to the criminal standard, that a defendant provided immigration advice and/or services. Secondly, a legal burden on a defendant in these circumstances does not impose an onerous obligation as he or she will be well aware of the route to qualification which required to satisfy the legislation and will have ready access to information or evidence to establish this qualification. Given there are various routes to qualification, it would be exceedingly complex for the prosecution to disprove qualification.[204]

104. In *R v.Johnstone,* the court considered section 92 of the *Trade Marks Act 1994* which creates the offence of being in possession of goods that

[200] *Sheldrake v. DPP* [2005] 1 AC 264, para 21
[201] *R v Roy Clarke,* [2008] EWCA Crim 893, at para 19, citing Lord Hope of Craighead
[202] *Ibid.,* at para 21
[203] *Ibid.*
[204] *Ibid.* pp. 26 - 30

infringe a registered trade mark punishable on indictment with up to 10 years' imprisonment. The House of Lords held that the reverse burden within section 92(5), creating a defence on proof that the defendant had a reasonable belief that the goods were not infringing, was proportionate on the basis that the facts were within the defendant's own knowledge, that he had engaged in trade in branded products knowing of the risk of counterfeit goods and that Parliament had primary responsibility for policy decisions as to the constituents of the offence.[205]

105. However, the courts have held reverse burdens to violate Article 6(2) in the certain cases. In *Attorney General's Reference (No 4 of 2002)*[206] the House of Lords considered s. 11(1) of the *Terrorism Act 2000* which creates the offence of being a member or professing to be a member of a proscribed organisation. Section 11(2) of that Act provided that it was a defence to prove that the organisation was not proscribed when the defendant became a member (or began to profess to be a member), and that he had not taken part in any of its activities while it was proscribed. The House decided, by majority, that although section 11(2) of that Act imposed a legal burden, it was disproportionate to the legitimate aim of the legislation and should be read down to being an evidential burden only.

106. The House of lords reached this decision for various reasons: firstly, the uncertain scope of the word "profess" within s.11(1) was such that a person who was innocent of criminal conduct could fall within s.11(1). There would be a clear breach of the presumption of innocence if such a person could exonerate himself only by establishing a defence on the balance of probabilities and it was the duty of the courts to protect defendants against such risk. Secondly, it might be impossible for a defendant to show that he had not taken part in the activities of the organisation at any time while it was proscribed. Thirdly, if s.11(2) imposed a legal burden there would be no room left for the courts to exercise a discretion. Finally, a conviction under s.11(1) could result in a sentence of 10 years' imprisonment. Consequently, the burden imposed by s.11(2) was not a proportionate or justifiable response to legitimate security concerns.[207]

Data offences and defences

107. A number of data offences are set out in the Bill. Some of the defences require the defendant to "prove" his defence.[208] The relevant offences are:

[205] *R. v.Johnstone,* [2003] 1 WLR 1736, cited in *R v Roy Clarke*, at para 21
[206] Reported with *Sheldrake v. DPP* [2005] 1 AC 264
[207] *Attorney General's Reference (No 4 of 2002)*
[208] Clauses 139, 160, 163, and 171 of the Bill

a) Failure to comply with an information notice (a notice that requires a controller or processor to provide the Commissioner with specified information within a certain period of time);[209]
b) Intentionally or recklessly making a false statement in response to an information notice;[210]
c) Unlawful (deliberate or reckless) obtaining, disclosing, or retaining of personal data without the consent of the data controller;[211]
d) Re-identification of de-identified personal data, knowingly or recklessly, without the consent of the controller who de-identified the data;[212]
e) Alteration of personal data to prevent disclosure following the exercise of a subject access right;[213]
f) Requiring employees/contractors/providers of goods, facilities or services to provide records obtained via a subject access request as a condition of their employment/contract.[214]

108. The defences to each of the above offences place a legal burden of proof upon the defendant by requiring him/her to prove his/her defence.[215] The Government justifies these burdens on three grounds:
a) the seriousness of the offences;
b) effective enforcement of data processing regulations; and
c) the non-custodial nature of the penalties.[216]

109. Whilst the Government's justifications would weigh in consideration, the courts would have to apply the principles set out in the case law above in order to assess whether it is necessary and proportionate to impose a legal rather than an evidential burden on an accused. The relevant offences and reverse burden defences are set out below.

110. Clause 139: The prosecution has to prove the defendant failed to comply with an information notice. The defendant has to prove, on the balance of probabilities, that he exercised all due diligence to comply with the notice.[217] The steps taken by the defendant in the exercise of his due diligence is something within his knowledge and arguably not difficult to prove.

111. Clause 161: The prosecution has to prove that the defendant deliberately or recklessly obtained, disclosed, or retained personal data

[209] Clause 139(1) of the Bill. This is a notice that requires a controller or processor to provide the Commissioner with specified information within a certain period of time. See clause 137.
[210] Clause 139(3) of the Bill
[211] Clause 161 of the Bill
[212] Clause 162 of the Bill
[213] Clause 163 of the Bill
[214] Clause 171 of the Bill
[215] Defences are set out in clauses 139, 161, 162, 163, and 171 of the Bill
[216] Explanatory Notes, para 805
[217] This replicates s.47 of the Data Protection Act 1998

without the consent of the data controller. There are two defences. Under sub-section (2) the defendant must prove that the purpose was the prevention or detection of crime, fulfilling a legal obligation, or the public interest. Under sub-section (3) the defendant must prove they reasonably believed they had a legal right or the consent of the data controller. The facts required to prove either defence are arguably reasonably within the knowledge of the defendant.

112. Clause 162 (1): The prosecution has to prove that the defendant knowingly or recklessly re-identified information that had been de-identified without the consent of the controller who de-identified the data. A defendant can raise two defences to this. The first defence requires him to prove that the re-identification was necessary for the prevention or detection of crime, fulfilling a legal obligation, or the public interest. The second defence requires the defendant to prove that he had a reasonable belief either that he had the consent of the data subject or the data controller, or would have had that consent had the controller known about the circumstances. Clause 162(5): The prosecution has to prove that the defendant knowingly or recklessly processing data that has been unlawfully re-identified. The defences are the same as those that apply under clause 162(1). The facts required to prove either defence are arguably reasonably within the knowledge of the defendant.

113. Clause 163: The prosecution has to prove that the defendant altered personal data to prevent disclosure following the exercise of a subject access right. The defendant is required to prove that the alteration either (a) would have occurred in the absence of a subject access request, or (b) he reasonably believed the person making the request was not entitled to receive the information. The facts required to prove either defence are arguably reasonably within the knowledge of the defendant.

114. Clause 171: The prosecution must prove that the defendant required employees/contractors/providers of goods, facilities or services to provide records obtained via a subject access request as a condition of their employment/contract. The defendant must prove that the requirement was required or authorised by an enactment, by a rule of law, or by order of a court, or in the particular circumstances it was justified in the public interest.

115. One of the key questions in assessing reasonableness of reverse burdens is whether they relate to something which is likely to be within the defendant's knowledge or to which the defendant has ready access. Most of the burdens appear to be reasonable, as they are likely to be within the defendant's knowledge, for example, the requirement upon the defendant to prove he had a reasonable belief in consent. However, it may be more difficult

to prove that something was required or authorised by an enactment or rule of law without legal knowledge, although this will depend upon the specific circumstances. Whether this is reasonable is likely to turn on the specific facts of the case.

b. Re-identification of de-identified data

116. The re-identification of de-identified data is a new criminal offence not included in the GDPR or the current DPA.[218] As explained by Lord Ashton of Hyde at Second Reading, datasets used by researchers and developers are often pseudonymised to protect individual privacy. This offence demonstrates that "we will not tolerate assaults on individual privacy, nor on the valuable data assets that are fuelling our innovative industries."[219] Tech UK has noted that there are already laws which prevent individuals from using personal data for reasons other than which it was collected, such as identity theft and fraud.[220] Under the GDPR, if personal data is used for a purpose for which it was not originally collected or processed, the data controller would have no legal basis for processing and would be in breach of the GDPR and liable to fines. Further, in some situations, re-identification of pseudonymous data may be legitimate and necessary such as when testing a security system to ensure it is effective. Tech UK therefore suggests, at a minimum, that research and security should be added as defences against this offence as important security research should not be prevented by this new offence.[221]

c. Rights to bring a claim and rights of appeal

117. Article 80(1) of the GDPR allows for representative bodies, such as consumer rights groups, to bring complaints where instructed by data subjects. Article 80(2) allows those groups to bring complaints where they believe data rights have been breached, without the instruction of a data subject. The purpose behind this is to give data subjects enhanced protection by allowing civil society groups to defend their rights without the need for the data subjects to exercise these rights. Article 80(2) is, however, an optional clause and has not been adopted in the Bill. Baroness Lane-Fox of Soho argued that this omission "places a huge onus on individuals, who may lack the know-how and the ability to fight for their rights….This omission is worrying, given how stretched the ICO's resources are and the impact this could have on its support for the public. Granting rights over data to individuals is meaningless if individuals lack the understanding to exercise

[218] Clause 162 of the Bill
[219] Lord Ashton of Hyde, Second Reading, Data Protection Bill [HL], 10 October 2017, Hansard Vol. 785, col.127
[220] Tech UK, Briefing on the Data Protection Bill for Second Reading, 10 October 2017, p10
[221] *Ibid.,* p10

those rights and there is no infrastructure within civic society to help them exercise those rights."[222]

118. Privacy and digital rights organisations have also expressed concern, pointing out that UK law provides for collective action under the *Consumer Rights Act 2015* and under the *Enterprise Act 2002* for any market failures that harm the interest of consumers, which ought to be replicated in the context of data protection under the Bill. Privacy International notes that "the imbalance of powers between powerful companies and data subjects makes it very difficult for individuals to effectively claim their rights, notwithstanding the important role played by the ICO in protecting personal data."[223] Privacy International therefore proposes an amendment to enable qualified NGOs to take up collective actions on behalf of citizens affected by data breaches.[224]

119. **The Committee may wish to consider whether the reverse burdens constitute a proportionate interference with Article 6(2) and whether a broader defence to the new 're-identification' offence is required. The Committee may also wish to consider whether the Government's omission of Article 80(2) may diminish the protection of privacy rights and, if so, whether civil society organisations ought to be empowered to bring complaints and seek effective remedies in the public interest.**

v. Rights of the child

120. The GDPR and the Bill contain provisions to enhance the protection of children's rights online in respect of their personal data. For example, where online services are offered to a child, privacy notices must be clear and comprehensible for children. Article 8 of the GDPR provides the age at which a child can consent to the processing of their data by online sites such as search engines and social media. The minimum age allowed by the GDPR is 13 and the maximum is 16. In clause 8, the Bill sets the age at 13. Children aged 13 and over would not therefore have to seek the consent of a guardian when accessing certain online services.[225]

121. Concerns have been raised about the low age of consent. In Committee stage debate, Lord Stevenson of Balmacara noted that no credible evidence had been adduced to support the decision, citing the Children's Commissioner for England who stated that: "the social media giants have …

[222] Baroness Lane Fox, Second Reading debate [HL], 10 October 2017, Hansard vol. 785, col. 158
[223] Privacy International, Briefing on the Data Protection Bill for Second Reading, 6 October 2017
[224] Privacy International, Written Evidence, DPB0004, p.12, para 3.3
[225] Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to children

not done enough to make children aware of what they are signing up to when they install an app or open an account…children have absolutely no idea that they are giving away the right to privacy or the ownership of their data or the material they post online".[226] Further, he cited The Children's Society which argued that if companies continue to rely on their current practices, whereby they allow only over-13s to have an account but have no age verification process to check that children who are consenting are the age they state themselves to be, then there will continue to be widespread breaches of both the companies' own rules and this new Act. It is unclear how breaches will be handled by the Information Commissioner and what penalties will be put in place for those companies failing to verify age properly. There is, therefore, a need both for proper evidence to be gathered and for a minimum requirement for companies to have robust age verification systems and other safeguards in place before any such legislation is passed.[227]

122. In written evidence, The Equality and Human Rights Commission (EHRC) submits that the fact that some companies use the age of 13 as the minimum age to offer services to children does not justify this as the default age in the Bill. Further, any educational needs of children to use online services could be met by an exemption. The EHRC argue that more work must be done to reach a justified conclusion on the right age of consent, taking into account the UK's obligations under the UN Convention on the Rights of the Child.[228] **The Committee may wish to consider whether the age of consent complies with the best interests of the child principle.**

V. Next steps

123. There are various human rights concerns to which the Committee may wish to give further attention. In particular, the Committee may wish to consider:

a) whether Article 8 of the Charter ought to be expressly included in the Bill;
b) whether an exemption for effective immigration control is necessary and proportionate given the broad reach this exemption would have;
c) whether automated decision-making requires further safeguards to ensure that decisions significantly affecting human rights are not being made on an automated basis;
d) whether the Bill provides sufficient clarity as to the meaning of "substantial public interest" and "public interest" and whether the safeguards for processing of "special categories data" are sufficient;

[226] Lord Stevenson of Balmacara, Second Reading debate [HL], 10 October 2017, vol. 785, col. 131
[227] *Ibid*.
[228] Equality and Human Rights Commission, Written Evidence, DPB0006, November 2017, p4 para ii

e) whether the powers contained within the Bill permitting cross-border transfers of data and the unfettered powers granted to the intelligence services in the absence of any safeguards are necessary and proportionate;
f) whether the broad and indefinite national security exemptions are necessary and proportionate and whether oversight for the issuing of national security certificates is sufficient;
g) whether the right of appeal against national security certificates provides an effective judicial remedy;
h) whether the significantly reduced safeguards for intelligence services are necessary and proportionate and whether there is sufficient oversight of the intelligence services given their broad and unfettered powers;
i) whether to engage with the Intelligence and Security Committee and the Independent Reviewer of Terrorism Legislation to explore further the matters concerning national security;
j) whether the delegated powers are necessary and proportionate in light of the breadth of the powers and the potential to remove rights without parliamentary scrutiny;
k) whether the reverse burdens constitute a proportionate interference with Article 6(2) ECHR and whether a broader defence to the new 're-identification' offence is required;
l) whether civil society organisations ought to be empowered to bring complaints and seek effective remedies in the public interest;
m) whether the age of consent complies with the best interests of the child principle.

124. **If the Committee wishes to take any of these matters forward, potential amendments could be explored before Christmas recess with a view to reporting in January 2018.**

Samantha Godec
Deputy Counsel