PRIVACY INTERNATIONAL

Briefing

Privacy International's briefing on the Data Protection Bill for Second Reading in the House of Lords

October 2017

About Privacy International

Privacy International (PI) was founded in 1990. It is a leading charity promoting the right to privacy across the world. It is based in London and, within its range of activities, investigates how our personal data is generated and exploited and how it can be protected through legal and technological frameworks. It has focused on the General Data Protection Regulation (GDPR) and its passage through the EU institutions since 2009. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

Contacts:

Anna Fielder
Senior Policy Adviser
Chair Emeritus
020 3422 4321
anna@privacyinternational.org

Tomaso Falchetta
Advocacy and Policy Team Lead
020 3422 4321
tomasof@privacyinternational.org

Introduction and summary of main concerns and recommendations

Privacy International welcomes the aim of this Bill (Data Protection Bill), "to create a clear and coherent data protection regime", and to update the UK data protection law, including by bringing the EU General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive (DPLED) - into the UK domestic system.

1. **Clarity and accessibility of structure** (page 3)
The Bill is overly and unnecessarily complex in its design and structure, which makes it opaque and inaccessible for organisations that cannot afford expensive lawyers. We recommend ways that structure can be simplified.

2. **Delegated powers** (page 4)
The Bill has many regulation making powers, and grants an unacceptable amount of power to the Secretary of State to introduce secondary legislation, bypassing effective parliamentary scrutiny. We recommend that the Bill is amended to limit such broad powers.

3. **Representation of living individuals** (page 5)
The Bill does not provide for qualified non-profit organisations to pursue data protection infringements of their own accord, as provided by EU General Data Protection Regulation in its article 80(2). We, along with UK digital rights and consumer organisations strongly recommend that the Bill is amended to include this provision.

4. **Conditions for processing special categories of personal data** (page 6)
There is no definition in the Bill of what constitutes "substantial public interest" when processing sensitive personal information, or why the 17 conditions for processing such information constitute such interest. This will result in lack of adequate safeguards to protect such sensitive data in all cases. We recommend that this concept is better defined and narrowly interpreted.

5. **Automated decision-making** (page 7)
Profiling and other forms of decision-making without human intervention should be subject to very strict limitations. The Bill provides insufficient safeguards for automated decision making. We recommend the Bill to be amended to include further concrete safeguards.

6. **National Security Certificates** (page 8)
Provisions in the Bill mirror those in the current Data Protection Act, but include even wider exemptions. Privacy International's concerns include the timeless nature of the certificates, lack of transparency, no means to challenge, and wide powers exempt from data protection principles. We make a number of concrete obligations to be included in the Bill.

7. **Intelligence Agencies, cross-border data transfers** (page 10)
The Bill provides for almost unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection; this is an infringement of the requirements of Council of Europe's modernised Convention 108. We recommend that rules for such transfers are brought into line with those required in the Bill for law enforcement purposes.

Main concerns and recommendations

1. Clarity and accessibility of structure

While acknowledging that the Data Protection Bill covers three distinct sectors (general, law enforcement and intelligence) and has to also anticipate the Brexit scenario, we think that it is overly and unnecessarily complex in its design and structure. This law needs to be accessible to thousands of small businesses, charities and public institutions who do not have the funds to pay expensive law firms to help them implement the legislation, and we are concerned that they cannot do that in its present format. The structure and language will also pose difficulties to individuals seeking to understand and exercise their rights under the Bill.

Our experience of research and work for many years is that "controllers", including public bodies, do not understand well their obligations under the current Data Protection Act 1998 (DPA); the proposed Bill is even more obscure.

Part 2

The distinction between GDPR and 'applied GDPR' is unclear and unhelpful. In particular it is not clear to which sectors and kind of processing of personal data Chapter 3 applies. The fact that Schedules are separated from the relevant provisions and that the provisions of the GDPR are not reproduced in the bill, not even as an annex makes it very difficult to follow it and understand.

- **We recommend** that clarity is provided on the rationale for the distinction between 'GDPR" and "applied GDPR' and on which activities fall outside the scope of EU law and are not covered by Part 3 or 4 of the Bill. An attempt should be made to simplify Part 2, thereby giving individuals and organisations a clearer understanding of their rights and obligations.

Part 3 and Part 4

There is no reason for separate regimes of data protection for law enforcement (Part 3) and intelligence agencies (Part 4.) We note the statement of the Minister of State for Security that GDPR and the LED "were not designed to be applicable to the unique nature of processing by the intelligence services" [1], however, no further reasoning for the different regime is provided.

For example, we are concerned that the data breach reporting requirements in Part 4 of the Data Protection Bill do not mirror those in Parts 2 and 3. We note that in clause 106 (7) of Part 4 there must be a serious interference with the rights and freedoms of a data subject before the breach is reported and that there is no obligation to report a breach to the data subject. Furthermore, in terms of enforcement, Part 4 is excluded from clause 158 (4) (b) of this Bill which means that individuals who consider their rights have been infringed cannot apply to a court for a compliance order. We are concerned that Part 4 does not provide an effective oversight regime for intelligence agencies and for

[1] See letter from Minister of State for Security to the Chair of the Intelligence and Security Committee http://data.parliament.uk/DepositedPapers/Files/DEP2017-0557/Min_for_Security_to_Chair_Intel_and_Security_Com_Data_Protection_Bill.pdf

this reason consider that such agencies covered by Part 4 should also fall within the ambit of Part 3 of the Data Protection Bill. This would still allow for the standards of protection in the modernised Council of Europe "Convention 108".

- We recommend that Parts 3 and 4 are combined and that in doing so the highest standards of protection (particularly in relation to the rights of living persons) are applied.

2. Delegated powers

We are concerned that the Data Protection Bill has many regulation making powers, and grants an unacceptable amount of power to the Secretary of State to introduce secondary legislation. This bypasses effective parliamentary scrutiny.

In particular, clause 15 gives the Secretary of State wide powers to alter the applications of the GDPR, including notably new legal bases to share personal information in the public interest or in the exercise of public authority, restricting the rights of individuals.[2]

We are also concerned with the regulation making power of the Secretary of State in clause 9(6) to amend Schedule 1 (conditions for processing special categories of personal data) by adding, varying or omitting conditions or safeguards, and to make consequential amendments of this section. We are concerned that this power is overly wide, and does not place sufficient importance on the prohibition on processing special categories of personal data in Article 9(1) of GDPR. We note the explanation provided in the Explanatory notes to the Data Protection Bill, that it is not possible to predict what future circumstances may arise which justify processing of these particularly sensitive categories of data without explicit consent. However, Schedule 1 to the Bill already provides for a large number of exemptions and any ability to amend the limited conditions in which special categories of personal data can be processed should have sufficient checks in place.

These concerns are compounded by the fact that the proposed European Union (Withdrawal) Bill gives "excessive wide law-making powers to Ministers".[3] This could include changing provisions currently in the GDPR, a prospect of great concern, also in light of the proposal contained in the EU Withdrawal Bill to end the application of the European Charter on Fundamental Rights and Freedoms, which includes the right to data protection in Article 8.

- We recommend that the Data Protection Bill is amended to include provisions to limit such broad regulation-making powers, including by: i) removing the ability of the Secretary of State to establish new legal basis for processing of personal data where processing is necessary for compliance with a legal obligation, for the performance of a task in the public interest or

[2] See also concerns expressed by O. Butler, 'The Data Protection Bill and Public Authority Powers to Process Personal Data: Resurrecting Clause 152 of the Coroners and Justice Bill 2009?', U.K. Const. L. Blog (28th Sept. 2017) (available at https://ukconstitutionallaw.org/)

[3] See Delegated Powers and Regulatory Reform Committee Third Report, https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/22/2202.htm

in the exercise of official authority, in clause 15 (1)(a); ii) removing the ability to omit safeguards in clause 9 (6) and iii) requiring open and transparent publication of draft regulations and provide for consultation from the ICO, the public and civil society.

3. Representation of living individuals

Together with other digital rights and consumer organisations, we are deeply disappointed that the Data Protection Bill does not provide for qualified non-profit organisations to pursue data protection infringements of their own accord (as provided in Article 80(2) of GDPR). Given that in the UK 'opt-out' collective action is already enabled under the Consumer Rights Act 2015 and under the "super-complaint system" (Enterprise Act 2002) for any market failures that harm the interest of consumers, we expected that such empowerment would be extended to data protection under the Bill, since personal data has become such an essential part of the national and global economy and it has often been noted how 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. We note that around Europe NGOs have successfully brought collective actions in past years under both consumer and data protection laws against powerful digital corporations to the benefit of all[4]. Both Germany and France are empowering qualified NGOs under the provisions of this Article, and Poland is currently consulting to do so.

- We recommend that the Data Protection Bill is amended to include the provision, as enabled by Article 80(2) of the GDPR, for a not-for-profit body which has statutory objectives in the public interest and active in the field of protection of individuals' personal data to, independently of a data subject's mandate, to have the right to lodge complaints with a supervisory authority, as well as seek effective judicial remedy when it considers that the rights of a data subject under the GDPR have been infringed.

4. Public interest test and conditions for processing special categories of personal data

Privacy International is concerned about the lack of definition of "substantial public interest" in relation to clause 9 (and Part 2 of Schedule 1) for the processing of special categories of personal data and we consider that it should be interpreted narrowly to ensure protection of the rights of individuals.

There is a lack of explanation in the Bill or the accompanying Explanatory Notes as to why it is considered that the 17 conditions for processing special categories of personal data contained in Part 2 of Schedule 1 are in the "substantial public interest".

[4] For e.g. German Consumer Federation vs Apple (2013, unfair contract terms); France, UFC – Que Choisir vs Google, Facebook and Twitter (2014, unfair contract terms and illegal practices in privacy policies); Europe vs Facebook case in Austria (2015 illegal privacy and data protection practices)

These conditions appear to have been for the most part transposed from Schedule 3 to the DPA, with little attempt to re-consider and reform them to reflect the changing way in which our sensitive personal data can be inferred and processed. Whist we welcome the requirement for an appropriate policy document and the additional safeguards in Part 4 of Schedule 1 and note the restrictions on automated decision-making in Article 22 of GDPR and clause 13 of the Bill, we do not consider these offer adequate safeguards to protect individual's sensitive personal data in the case of every exemption.

For example, paragraph 17 of Schedule 1 to the Bill permits registered political parties to process personal data revealing political opinions for the purposes of their political activities. This can include, but is not restricted to, campaigning, fundraising, political surveys and case-work. 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).[5] 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.

More generally, we are also concerned at the lack of clarity around the definition of "public interest" throughout the Data Protection Bill and how this is to be interpreted in practice. For instance, clause 7 of the Bill contains a non-exhaustive list of examples to illustrate lawfulness of processing as a way to implement Article 6(1)(e) of the GDPR. Whilst we recognise that these are public interest provisions also in the DPA, this does not excuse the need for further clarification of this point in order to inform both data controllers and data subjects and assist them in exercising their obligations and rights contained in GDPR and the Data Protection Bill.

- We recommend that the Data Protection Bill restates that "Member State law shall meet an objective public interest and be proportionate to the legitimate aim pursued", as per Article 6(3) of GDPR.

- We recommend that further clarification on the scope of "public interest" and of "substantial public interest" is provided, if not in legislation, then in guidance from the ICO, as this is extremely relevant to many areas of the Bill. For example, in the context of freedom of information legislation, both the UK ICO and the Scottish Information Commissioner have provided guidance on the application of the public interest test.

6. Automated decision-making

The right not to be subject to automated decision-making is a fundamental provision in the GDPR. Privacy International believe that profiling and other

[5] See Privacy International, Cambridge Analytica Explained: Data and Elections, https://www.privacyinternational.org/node/1440

forms of automated decision making should be subject to very strict limitations and allow individuals the right not to be subjected to a decision based on automated processing without their fully informed and explicit consent.

We consider that the safeguards provided in clause 13 of the Data Protection Bill, in accordance with Article 22(2)(b) of the GDPR, are insufficient, notably under clauses 13(4)(a) and (5) (a) the obligation to notify, and a right to reconsideration of the decision, or a new decision, do not adequately safeguard the rights, freedoms and legitimate interests or data subjects. For example, there is no right to complain to a relevant authority, or seek judicial redress regarding a decision based solely on automated processing.

The option for the Secretary of State to make regulations providing further provision as to appropriate safeguards provides no guarantee or clarity on any further safeguards.

We have similar concerns in relation to clauses 47 and 48 (law enforcement processing) and clauses 94 and 95 (processing by intelligence agencies.)

- We recommend that the Data Protection Bill is amended to provide further concrete safeguards regarding automated decision-making authorised by law, such as full information about the logic involved and likely consequences of the decision (cf. Article 13(2)(f) of GDPR), as well as a right to complain, and to seek judicial redress.

- The Data Protection Bill does not provide any information on which laws may currently require or authorise such automated decision making. As such we recommend that during the consideration of this Bill, the government is required to provide a list of laws that allow for automated decision-making.

7. Exemptions for national security - National Security Certificates

Privacy International is concerned by the national security exemption provisions contained in Part 2 Chapter 3 ('applied GDPR', clauses 24 - 25), Part 3 Law Enforcement Processing (clause 77) and Part 4 Intelligence Services Processing (clauses 108-109).

To a large extent this mirrors the provisions in section 28 of the DPA, which provide already for extremely wide exemption from the DPA where a national security certificate has been made, although the Data Protection Bill appears to expand it even further, in particular the inclusion of a 'defence' exemption in the 'applied GDPR'. No definition has been provided for the defence exemption nor clarification in the Bill or explanatory notes as to what this covers.

Our concerns are based on the present scheme for national security certificates under the DPA. In particular we are concerned about:

<u>Wide powers to exempt from data protection principles and rights</u>
There are common themes to the issuance of national security certificates that have come to light according to information obtained by Privacy International: a complete exemption of the first, second and eighth principles, the section 55

offence of unlawfully obtaining personal data, commissioner's powers of enforcement and the rights of access and objection.

The Data Protection Bill offers the possibility to exempt data processors from a wide range of principles and rights:

- Under 'applied GDPR' (clause 24) which includes inter alia all rights of the data subject;
- Under law enforcement (clause 77) which includes "any restriction to which it relates by means of a general description";
- Under intelligence agencies (clause 109) which includes all rights of the data subject and most of the data protection principles.

It is unclear why these authorities would need to be exempted from so many obligations under the data protection regime, including in relation to the rights of data subjects; the responsibilities of data controllers and processors; and to safeguards for transfers of personal data to third countries and international organisations. We believe public trust in effective data protection will be undermined as a result.

- We recommend that the Data Protection Bill provides that, at the very least, the following obligations should always be upheld: processing of personal data lawfully and ensure that any processing is necessary for fulfilment of statutory functions; processing personal data for a specified and lawful purpose; ensuring that personal data are processed in a way that is not incompatible with the national security purpose; ensuring that all personal data are adequate, relevant and not excessive in relation to the national security purpose; ensuring personal data shall be accurate, particularly in the age of automated decision making and use of artificial intelligence techniques; ensuring that personal data are kept no longer than necessary for the national security purpose; ensuring that personal data be kept secure; ensuring that personal data are not to be transferred to a country that offers an inadequate level of protection unless there is a substantial public interest in any transfer.

<u>Timeless nature of the certificates and lack of transparency:</u>
Certificates are timeless in nature. Once they are signed by the relevant Cabinet Minister, they exist for all-time, unless they are reviewed.[6]

There is no transparency as to what Certificates are currently in place for law enforcement; intelligence agencies; government departments; private companies and other organisations.[7]

- We recommend disclosure of all Certificates currently in existence in order to effectively scrutinise this secretive regime. We further

[6] Example of timeless nature: In Privacy International's litigation regarding bulk data, the Agencies relied upon certificates signed by David Blunkett and Jack Straw in 2001 to exempt key obligations in the Data Protection Act for activities which commenced several years later. https://www.privacyinternational.org/node/938

[7] We are aware of certificates in relation to the Intelligence Agencies, Intelligence and Security Committee and Transport for London.

recommend that the Bill requires that any certificate issued under the bill is made publicly available.

Inability to challenge:
Under section 28 of DPA if a person wants access to her data but a certificate is issued, she would get the response "we have given you all that is required under the Act." There would be no mention that information has been withheld on grounds of national security. The same is true of the provisions in the Data Protection Bill. That makes it difficult for the individual to appeal the notice because the legislation states that she may only do so if she is "directly affected" by it, and at that stage she does not know whether or not she is.

In addition, whilst a person directly affected by the issuing of any certificate may appeal to the tribunal to judicially review the decision to issue the certificate it is unclear how any challenge process could work if there is no public record of certificates and no way a data subject can know whether the national security exemption has been applied to their access rights. Further, even should an individual seek to bring a challenge, the provision for judicial review is insufficient as too narrow, prohibitively costly and complex.

As for the power of the Commissioner, the Data Protection Bill does not contain exactly the same provision as section 51 of DPA. In particular it is unclear whether the Commissioner would have the same power to challenge a national security certificate in the Tribunal, as under the DPA.

- We recommend that the right to challenge the national security certificate is strengthened, including by amending clause 25(3), clause 77(5) and clause 109(3) to ensure that any person **who believes they are** directly affected by a certificate may appeal to the tribunal. This will bring these clauses into line with section 65 in RIPA.

8. Transfer of personal data outside the UK by intelligence agencies

We are particularly concerned by clause 107 on transfers of personal data outside of the United Kingdom by intelligence agencies.

This clause provides almost unfettered powers to transfer personal data, the only condition being that such transfers are necessary and proportionate for the purposes of the controller's statutory functions or for other purposes as provided in the Security Service Act 1989 or Intelligence Services Act 1994. As such purposes are significantly broad, this clause fails to provide any meaningful safeguards to the sharing of personal data.

As such this clause provides for no requirement of appropriate level of protection as demanded by Article 12 of the Council of Europe modernised "Convention 108" which this clause is said to implement.

Privacy International notes, as a general matter, that intelligence sharing arrangements are typically confidential and not subject to public scrutiny, often taking the form of secret memoranda of understanding directly between the

relevant ministries or agencies. The U.N. Special Rapporteur on Counter-Terrorism has stated in this regard that:

"*The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority. Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards […] Such practices make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the [International] Covenant [on Civil and Political Rights]."*[8]

The European Court of Human Rights has also expressed concerns regarding the practice of intelligence sharing.[9]

Just as government surveillance must be transparent and subject to adequate safeguards and oversight, so too must intelligence sharing arrangements. Non-transparent, unfettered and unaccountable intelligence sharing threatens the foundations of the human rights legal framework and the rule of law.

Domestic legislation governing intelligence sharing is inadequate.[10] There are multiple ways in which data may be shared:

- The third party is given the ability to access (directly or remotely) material intercepted by the Agencies, which the third party can then process, store and/or disseminate further.
- The third party is given the ability to access remotely the Agencies' own databases, allowing for querying and search of those databases: a legal analogy would be giving someone a username and password for Westlaw or LexisNexis, allowing for searches of a database held elsewhere.
- The third party receives a copy of the data which has been selected for sharing: a legal analogy might be giving someone a copy of the entire set of the Law Reports.

It is unclear whether transfers in the Data Protection Bill cover all of the above or just the third category. In the modern era, it is imperative that all types of transfers are subject to the Data Protection Bill. These methods of sharing each carry distinct but overlapping risks:

- Permitting direct or remote access to raw intercept material allows the third party unfettered access to data obtained by the Agencies at the point of collection, which they may then process, store and/or disseminate further.

[8] Report of the U.N. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397, para. 44 (23 Sept. 2014).
[9] See Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment, para. 78 (12 Jan. 2016).
[10] Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Ors [2016] UKIPTrib 15_110-CH

- Permitting remote access to the Agencies' own databases allows the third party to quickly search vast quantities of data which remain on the Respondents' systems. The third party gets all the benefits of access to the Agencies' systems and the power and intrusiveness of access to indexed and searchable material, without having to process the data itself.
- Transfer results in the data controller losing control of how the data is used, stored, retained, disclosed or destroyed.

The Intelligence Agencies have avowed that they use of the second and third methods in the course of Privacy International's litigation concerning bulk data.[11] All three categories of sharing are also the subject of Privacy International's litigation concerning UK bulk interception and UK access to data collected under US bulk surveillance programs.[12]

In Privacy International's litigation on bulk data,[13] where the legality of transfer and sharing of data is the subject of court proceedings in October 2017, it is argued that there is little, if any, oversight by the Commissioners in respect of the transfer of bulk data or remote access to it. It is unclear whether the use of shared data is even auditable or audited in fact. There is nothing in the Intelligence Services Commissioner's reports that indicates that any audit or analysis of what data has been shared has taken place.

Noting the submissions above regarding national security certificates, these have been used by the Agencies to abrogate the application of the eighth data protection principle under the DPA which provides 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." There is no secondary legislation or Code of Practice providing safeguards over the sharing of bulk data.

In separate litigation[14] challenging UK bulk interception and UK access to data collected under US bulk surveillance programs, Privacy International submit that in relation to communicating intercepted material to other parties, under section 15(2) RIPA, the Secretary of State is simply required to ensure that the disclosure of section 8(4) intercepted material "is limited to the minimum that is necessary for authorized purposes." Those authorized purposes (section 15(4)) are broadly drawn and do not limit the power to disseminate intercepted material to situations where there is a reasonable suspicion that an individual has committed or is likely to commit a criminal offence or is a threat to national security. The section 15(2) limitation does not apply to dissemination of intercepted material to foreign authorities (section 15(6)). The Independent Reviewer of Terrorism has noted, in this respects, that there is *"no statute or*

[11] Para 78- 86, see: http://bit.ly/2f0Knxm

[12] 10 Human Rights Organisations v. the United Kingdom, App. No. 24960/15, European Court of Human Rights.

[13] Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Ors [2016] UKIPTrib 15_110-CH Bulk Personal Datasets and Bulk Communications Data.

[14] 10 Human Rights Organisations v The United Kingdom, Application Number: 24960/15.

Code of Practice governing how exchanges [to foreign authorities] should be authorized or take place."[15]

Privacy International noted in its response to the consultation on the Draft Codes of Practice for the Investigatory Powers Act that very little attention was paid to intelligence sharing and the safeguard that must attach when data is shared. We noted the deficiency in the Codes and the Act itself. [16]

The UK legal regime on intelligence sharing lacks the required minimum safeguards. The provision in this Bill fails to bring it to conformity with standards complying with human rights law.

- We recommend that the regime of transfer of personal data outside the UK by intelligence services is strengthened and at least brought into line with the regime of transfer of personal data with third countries contained in Part 3 (law enforcement).

[15] David Anderson, Q.C., A Question of Trust, Report of the Investigatory Power Review, para 7.66.

[16] Privacy International's submission on consultation on the draft Codes of Practice, http://bit.ly/2xSzBgM