PRIVACY INTERNATIONAL

Briefing on the Data Protection Bill: Second Reading in the House of Commons

February 2018

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:

Camilla Graham Wood
Legal Officer
020 3422 4321
camilla@privacyinternational.org

Ailidh Callander
Legal Officer
020 3422 4321
ailidh@privacyinternational.org

Tomaso Falchetta
Head of Advocacy and Policy Team
tomasof@privacyinternational.org

Anna Fielder
Senior Policy Advisor and Chair Emeritus
anna@privacyinternational.org

Table of Contents

1 Summary 4

2. Key concerns 6

3. Delegated powers 8

5. Exemptions/ conditions for processing open to abuse 11

6. Automated decision-making 15

7. National Security Certificates 17

8. Intelligence agencies - cross border transfers 23

1 Summary

1.1. Privacy International welcomes the aim of the Data Protection Bill "to create a clear and coherent data protection regime", and to update 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.

1.2. A strong data protection framework is essential for the protection of human rights (including the right to privacy). It is also key to the granting of adequacy by the EU Commission following the UK's exit from the European Union.

1.3. However, the Bill falls short in the protections it provides in a number of areas. Privacy International has highlighted these concerns in our briefings during the consideration of the Bill in the House of Lords, at 2nd Reading, Committee and Report stage.[1] A number of Privacy International's concerns were reflected in the Note from the Deputy Counsel to the Joint Committee on Human Rights.[2] Many of our concerns and recommendations were raised by Peers at the House of Lords Committee stage and, as a result, some amendments to the Bill were introduced, most notably to provide better transparency of national security certificates. Notwithstanding, on key topics, the current version of the Bill still falls short of what should be expected from modern data protection legislation.

1.4. This updated briefing summarises our previous submissions and highlights our current key concerns as the Bill progresses through the House of Commons.

---

[1] See Privacy International's briefings for the Second Reading in the House of Lords (https://www.privacyinternational.org/advocacy-briefing/677/privacy-internationals-briefing-data-protection-bill-second-reading-house); Committee Stage re General Processing (https://www.privacyinternational.org/advocacy-briefing/656/privacy-internationals-briefing-data-protection-bill-committee-stage-house); and Committee Stage re Law enforcement and Intelligence services processing (https://www.privacyinternational.org/advocacy-briefing/627/briefing-data-protection-bill-committee-stage-house-lords-law-enforcement-and); and Report Stage https://www.privacyinternational.org/report/1639/privacy-internationals-briefing-uk-data-protection-bill-house-lords-report-stage

[2] http://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

1.5. References are to the Data Protection Bill [HL] [as amended on Report][3].

[3] https://publications.parliament.uk/pa/bills/lbill/2017-2019/0077/18077.pdf

2. Key concerns:

2.1. **Delegated powers:**
The Bill has many regulation making powers, and, despite some minor improvements during its House of Lords Passage, still 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. Amendments are needed to **Clauses 10, 16, 35, 86, 113 and 179** to address these concerns.

2.2. **Representation of living individuals:**
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 (GDPR) 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 to ensure data breaches, dangerous security flaws and unlawful conduct are remedied in an effective and efficient manner. Amendments are needed to **Clause 183** to address these concerns.

2.3. **Exemptions/ conditions for processing open to abuse:**
We have specific concerns regarding some of the wide-ranging conditions for processing and exemptions to the obligations and rights in the Bill/ GDPR, in particular in relation to immigration, political parties and the intelligence services. We recommend that these be narrowed or removed. Amendments are needed to **Paragraph 18 of Schedule 1, Paragraph 4 of Schedule 2, and relevant paragraphs in Schedules 9 and 11 as they refer to Part 4** to address these concerns.

2.4. **Automated decision-making**:
Automated decision-making without human intervention should be subject to very strict limitations to address issues of fairness, transparency, accountability and discrimination. The Bill provides insufficient safeguards. We recommend the Bill to be amended to include further concrete safeguards. Amendments are needed to **clause 14 (Part 2, general processing); clauses 49, 50 (Part 3, law enforcement); and clauses 96, 97 (Part 4, intelligence services)** to address these concerns.

2.5. **National Security Certificates**:
There have been modest improvements addressing the lack of transparency however, Privacy International maintains strong concerns about the broad and indefinite nature of national security exemptions; whether they are necessary and proportionate; whether oversight for issuing of national security certificate is sufficient; and whether the right of appeal against national security certificates provides an effective judicial remedy. We want concrete safeguards to be included in the Bill. Amendments are needed to **clauses 26, 27, 28 (Part 2, general processing), clause 79 (Part 3, law enforcement) and clauses 110, 111 (Part 4, intelligence services)** to address these concerns.

2.6. **Intelligence Agencies, cross-border data transfers**:
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. Amendments are needed to **clause 109** to address these concerns.

3. Delegated powers

3.1. The Bill has many regulation making powers, and grants an unacceptable amount of power to the Secretary of State to introduce secondary legislation.

3.2. Concerns with the delegated powers were flagged in reports by the Delegated Powers and Law Reform Committee and the House of Lords Select Committee on the Constitution.[4] As noted by Peers during the Bill's passage through the Lords, convenience and future proofing do not justify these "Henry VIII clauses" which are inherently undemocratic, remove parliamentary oversight and empower the executive to take away the rights of individuals without the checks and balances afforded to primary legislation through the parliamentary process.

3.3. These concerns are compounded 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.

3.4. Further, any future changes weakening the protections afforded by GDPR could impact on a future adequacy decision by the European Commission on whether the UK offers an adequate level of protection to allow processing of personal data from the EU. Effective parliamentary scrutiny is therefore essential.

3.5. During the passage of the Bill through the House of Lords limited amendments were made to delegated powers provisions. These changes do not address the concerns raised, as the Bill still provides for the Secretary of State to **add (and vary)** exemptions to data protection rights and obligations and **(add (and vary))** conditions for processing sensitive (special category) personal data. Removing or limiting protections for personal data and increasing the situations in which people's most sensitive personal data can be processed, risks undermining the very nature of data protection and any such amendments must be subject to parliamentary scrutiny.

[4] Report by the Delegated Powers and Law Reform Committee 9th Report available at: https://publications.parliament.uk/pa/ld201719/ldselect/lddelreg/48/48.pdf and Report by the Lords Select Committe on the Constitution 6th Report available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldconst/31/31.pdf

3.6. We recommend that the Bill is amended to (i) remove or limit such broad regulation-making powers as contained in clauses 10(6), 16, 35(6), 86(3), and 113 to address these concerns; and (ii) to require open and transparent consultation of draft regulations.

4. Representation of data subjects (Clause 183)

4.1. In order to protect and uphold the right to privacy and data protection, individuals need effective remedies when their rights are infringed. The Data Protection Bill in its latest version does not implement the GDPR Article 80.2 (optional) provision for qualified non-profit organisations to pursue data protection infringements on their own initiative – known as collective redress. As it stands, Clause 183 of the Data Protection Bill, enables individuals only to request such organisations to take up cases on their behalf, implementing the mandatory GDPR Article 80.1.

4.2. This is despite the Government's pre-Bill publication promise to enhance people's enforcement of rights, and despite the many solid arguments put forward by Labour, Liberal Democrat and Cross-bench peers in favour of such a clause. Debates around this clause and its value in terms of upholding data protection rights and controller accountability have been some of the most extensive at all stages of the passage of the Bill through the House of Lords

4.3. The Government, as a result, while rejecting all proposed amendments, has made a small concession, namely to introduce an amendment in the House of Commons, allowing for a review of how data subjects have made use of Clause 183 as it stands, two years after Royal Assent.

4.4. We think that a review of a clause in the Bill that does allow for collective redress would be more effective: weak enforcement provisions were one of the widely acknowledged reasons why the current data protection laws, in the UK and elsewhere in Europe, were no longer fit for purpose in the big data age. Due to power imbalances and information asymmetries between individuals and those controlling their personal information, data subjects remain as

unlikely to take up cases under the new laws in the future as they did in the past, notwithstanding enhanced enforcement rights.

4.5. Many data protection unlawful practices take place unseen, and can only be revealed by independent research and investigations, most often carried out by civil society organisations and charities. A recent example, in February 2018, comes from Germany where civil society organisations have been given some of these rights. The German Consumer Federation has taken Facebook to court over a number of the giant media platform's breaches of current German Data Protection Legislation; the final Court judgement upheld the majority of the consumer organisation's claims, including unlawful terms and conditions and consent provisions in its default privacy settings.[5]

4.6. Together with other digital rights and consumer organisations, Privacy International is deeply disappointed that clause 183 of the Data Protection Bill does not provide for qualified non-profit organisations to pursue data protection infringements of their own accord. 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 and should also be available in relation to data protection violations.

4.7. 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 is active in the field of protection of individuals' personal data to, independently of a data subject's mandate, 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.[6]

[5] English press release available to download at https://www.vzbv.de/pressemitteilung/facebook-verstoesst-gegen-deutsches-datenschutzrecht

[6] For further examples and arguments in favour of introducing collective redress provisions in Clause 183 see https://medium.com/@privacyint/why-we-need-collective-redress-for-data-protection-863c6640689c

5. Exemptions/ conditions for processing open to abuse

5.1. The GDPR allows Members States some discretion in defining the conditions for processing personal data and exemptions from data protection rights and obligations. However, the Bill includes conditions for processing special categories personal data and wide exemptions to data protection that undermine the right to privacy and the essence of data protection. These conditions/ exemptions lack justification, are poorly defined and broad in nature, therefore leaving them open to misinterpretation and abuse by those processing personal data.

5.2. In particular, we consider amendments need to be made to the following clauses:

- Remove or at least improve provision for processing by political parties of personal data revealing political opinions (**paragraph 18 of Schedule 1** of the Bill);
- Remove the exemption for processing personal data for effective immigration purposes (**paragraph 4 of Schedule 2** of the Bill);
- Restrict conditions and exemptions provided to the Intelligence Services (in **paragraph 6 of Schedule 9 and paragraphs 1, 10,12, 13 and 14 of Schedule 11 related to Part 4 of the Bill**).

Conditions for processing special categories of personal data - political parties (Paragraph 18 of Schedule 1 -)

5.3. Of particular concern is paragraph 18 of Schedule 1 to the Bill which permits registered political parties to process personal data 'revealing political opinions' for the purposes of their political activities. Political activities can include, but are not restricted to, campaigning, fundraising, political surveys and case-work. Whilst a variation of this condition was included in a statutory instrument to the Data Protection Act 1998, technology and data processing in the political arena have moved on. 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).

5.4. The granularity of data available for political campaigning and the practice of targeting voters with personalised messaging has raised debates about political manipulation and concerns regarding the impact of such profiling on the democratic process in the UK and elsewhere.[7] However, unlike party-political broadcasts on television, which are monitored and regulated, personalised, targeted political advertising means that parties operate outside of public scrutiny. They can make one promise to one group of voters, and the opposite to another, without this contradiction being ever revealed to either the voters themselves, the media or regulators. This happened in Germany for example, where the Afd radical party publicly promised to stop sharing offensive posters, yet continued to target specific audiences with the same images online.[8] In the UK, the Information Commissioner has commenced a formal investigation into the use of analytics by political parties following the EU Referendum and the 2017 General Election campaigns.[9]

5.5. It is essential that consideration is given to the way in which this condition for processing can interfere with the right to privacy and freedom of expression, particularly in light of technological developments and the granularity of processing of personal data. If your online activities and behaviour are used to profile you and reveal information as to your political opinions and this can then be used by political parties to target you for unlimited political activities, including fundraising, then this may result in a chilling effect on those seeking and imparting information in an online environment.

5.6. Whilst political parties' engagement with voters is a key part of a healthy democracy there are other conditions that political parties can rely on for processing and as a very minimum this condition must

---

[7] See Privacy International, Cambridge Analytica Explained: Data and Elections, available at https://www.privacyinternational.org/node/1440 and also see page 38, How Companies Use Personal Data Against People. Automated Disadvantage, Personalised Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information, Working paper by Cracked Labs, October 2017. Author: Wolfie Christl. Contributors: Katharina Kopp, Patrick Urs Riechert, available at: http://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf

[8] This became known only because NGOs asked voters to screenshot the ads

[9] See ICO blog of 17 May 2017 and updated of 13 December 2017 , available at: https://iconewsblog.org.uk/2017/12/13/update-on-ico-investigation-into-data-analytics-for-political-purposes/

be accessible and foreseeable in its terms to prevent abuse and interference with human rights.

5.7. Paragraph 18 should be removed from the Bill or at the very least amendments made to ensure that the scope of the condition is proportionate and adequate safeguards are established.

Immigration exemption (Paragraph 4 of Schedule 2)

5.8. The Bill contains a new and extremely concerning exemption for the purposes of 'effective immigration'. This is a broad and wide-ranging exemption which is open to abuse and interferes with human rights. This exemption should be removed altogether as there are other exemptions within the Bill that the immigration authorities can seek to rely on for the processing of personal data in accordance with their statutory duties/ functions or in the case of an offence. Such a broad ranging exemption which can impact substantially on human rights may also impact on an adequacy decision from the European Commission going forward.

5.9. To date, the Government has failed to offer any reasonable justification for the inclusion in the Bill of this new and wide-ranging exemption to the rights of data subjects.

5.10. Concerns about this exemption were raised strongly by the Lib Dem peers in the Lords and by other commentators, including civil society, academics and in the press by Labour MEP (and Chair of the European Parliament Committee on Civil Liberties, Justice and Home Affairs) Claude Mores, and Diane Abbott, Shadow Home Secretary.[10] We support other civil society organisations who are also pushing for the removal of this exemption, in particular, we would refer to Liberty's detailed briefing.[11]

Exemptions for processing by Intelligence Services (Part 4)

[10] See 'New UK data protection rules are a cynical attack on immigrants' 5 February 2018, available at: https://www.theguardian.com/commentisfree/2018/feb/05/brexit-data-protection-rules-immigrants

[11] https://www.liberty-human-rights.org.uk/sites/default/files/Libertys%20Briefing%20on%20the%20Data%20Protection%20Bill%202017%20for%20Report%20Stage%20in%20the%20House%20of%20Lords.pdf

5.11. The UK Intelligence Services must comply with the UK's human rights obligations and any interference with human rights such as the right to privacy and the right to freedom of expression must meet the requirements of being in accordance with the law, necessary and proportionate for the pursuant of a legitimate aim. Wide conditions for processing and broad exemptions in the Bill, do not meet these standards. Furthermore, there is a risk that these provisions taken together with the national security certificates and cross-border transfer provisions for intelligence agencies, could impact on a UK adequacy decision from the European Commission post Brexit given that factors looked in determining adequacy, as set out in Article 45 of GDPR, include respect for human rights, legislation concerning public security, defence and national security and the access of public authorities to personal data.

5.12. Of particular concern is, Paragraph 6 of Schedule 9 which permits the processing of personal data when it is in the interests of the intelligence agencies or the third party or parties to whom the data is disclosed. Unlike for private sector data controllers, public authorities and competent authorities (law enforcement) are unable to process personal data on the basis of a legitimate interest in processing. That is because they are already permitted to process personal data if it is within their statutory duties. This condition should be removed and intelligence services should be required to comply with the same standards as other public bodies.

5.13. **Schedule 11** of the Bill also provides a raft of broad exemptions for the intelligence agencies which also need to be revised and narrowed to ensure compliance with human rights and data protection standards.

6. Automated decision-making

6.1. The prohibition on certain forms of automated decision-making and the safeguards around this is an essential provision in GDPR. Automated decision-making without meaningful human intervention should be subject to very strict limitations. The Bill provides insufficient safeguards in this respect.

6.2. With technological advancements automated processes look set to play an increasing role in decision-making, this can have significant and lasting implications for an individual's human rights. Reliance on computational algorithms and machine learning poses a number of challenges, including with regards to opacity and auditability of the processing of data as well as accountability for decisions.

6.3. For data protection legislation to try to address the technological challenges that exist now and that lie ahead, the law must seek to ensure that profiling and automated decisions it informs are legal, transparent, fair, accountable and not discriminatory, and that data subjects can exercise their rights effectively.

6.4. Automated decision-making by public authorities must be subject to strict limitations and strong safeguards, especially in a law enforcement context where a potential miscarriage of justice can impact on an individual's wellbeing for life. Concerns about automated decision-making have been echoed in the press by Diane Abbott, Shadow Home Secretary.[12] Research by Privacy International has found that Police forces across the UK are already using or planning on using technologies which use opaque algorithms to predict crime and make decisions about individuals.[13]

6.5. The Article 29 Working Party (which brings together EU Data Protection Authorities, including the ICO) has issued guidance on

[12] See 'The Tories claim the data protection bill will make us safer. That's not true' 19 February 2018, available at: https://www.theguardian.com/commentisfree/2018/feb/19/tories-data-protection-bill-safer

[13] See Annex E of Privacy International's briefing on Law Enforcement and Intelligence Services for the Committee Stage of the House of Lords, available at: (https://www.privacyinternational.org/node/1550

Automated Decision-making and Profiling[14], which makes clear that Member State law that authorises automated decision-making must also incorporate appropriate safeguarding measures. As well as human intervention (as provided for in the Bill through the right to obtain a new decision not based solely on automated decision-making), the Guidance emphasises the need for transparency about the decision to the data subject and the ability of the data subject to challenge the decision.

6.6. We recommend the Bill be amended to include further concrete safeguards. Safeguards should include a meaningful right to explanation; a requirement for meaningful human involvement in certain decisions; and a right to complain and seek effective judicial redress as a result of the consequences of an automated decision. This following clauses need amended: 14 (Part 2, general processing); 49, 50 (Part 3, law enforcement); and 96, 97 (Part 4, intelligence services.)

[14] Article 29 Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, available at: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826

7. National Security Certificates

7.1. The Bill permits the use of national security certificates to exempt processing from key rights and duties under the Bill.

7.2. National security certificates have received insufficient scrutiny regarding their impact on privacy in the almost 20 years since the Data Protection Act 1998 was enacted. This is despite huge advancements in technological capabilities which have increased Government and corporate entities ability to collect and store personal data. No consideration has been given to the deleterious impact of exempting wholescale, vast amounts of data from data protection safeguards relying upon national security certificates.

7.3. The only amendment to national security provisions in the draft Bill in the House of Lords is the addition of clause 130.

7.4. Clause 130 introduces the ability for the Commissioner to receive a copy of certificates which have been issued under clauses 27, 79 and 111. This addition therefore does not address concerns over the opaque nature of the procedure by which certificates are issued, nor introduce effective independent oversight.

7.5. This limited amendment seeking to address transparency post-issue, is qualified in that publication is not permitted if deemed against the interests of national security; contrary to the public interest; or might jeopardise the safety of any person. Given the nature of these certificates, the likelihood is one against publication, which makes this provision ineffective.

7.6. The Bill continues to fail to address key concerns as to transparency over and accountability for the procedure for issuing of national security certificates. Further, the Bill appears to exacerbate concerns which existed in relation to section 28 of the Data Protection Act 1998.

7.7. National Security Certificates currently falls under section 28 of the Data Protection Act 1998, which changes the right of appeal against a decision from one of independent merits review to one in which the Tribunal merely determines whether the Minister was reasonable in his decision to issue a certificate.

7.8. There are a number of problems with the current regime. The ability to appeal against a section 28 national security certificate on judicial review grounds may only be of some assistance if the data subject and/or an appropriate body is aware of (a) the existence of the certificate, and (b) the reliance placed on the certificate. There is no process to subject certificates to scrutiny by Parliament or any other appropriate body. Clause 130 in the Bill is not a procedure whereby the national security certificate is subject to scrutiny and as noted the figleaf of transparency by publication is likely to be ineffective.

7.9. The Information Commissioner does not have an automatic role in scrutinising the validity of certificates as issued. Certificates may provide that the Information Commissioner's enforcement powers do not apply (*R (Secretary of State for the Home Department) v Information Tribunal and another* [2006] EWHC 2958 (Admin); [2008] 1 W.L.R 58)[15].

7.10. In many cases, data controllers (especially government agencies and departments) issue a mere neither confirm nor deny ("NCND") response to a data subject access request - without explaining that in doing so they are relying on a national security certificate. This leaves the data subjects with no indication of (i) whether their rights are affected at all and (ii) the right appeal route.

7.11. Unlawful certificates have been issued as where external scrutiny has taken place some certificates have been struck down (*Norman Baker MP v SSHD* [2001] UKHRR 1275)[16].

7.12. The impact of a section 28 certificate is significant. It limits the scope of appeal granted to the individual data subject - who may not even be told that a certificate is being relied upon.

---

[15]In response to the Commissioner's efforts to have access to the data held to permit her to perform her statutory role, the Department obtained a ministerial certificate signed by Rt Hon David Blunkett MP. The certificate stated essentially that no further disclosure should be made to the Information Commissioner because of national security concerns.

[16] In *Norman Baker MP v SSHD* [2001] UKHRR 1275, the relevant Information Tribunal found that a section 28 certificate applying in effect a blanket exemption to data subject access requests made in respect of files held by MI5 was unreasonably wide. This appeal was only possible because in that case the MP was aware of the reliance placed on the national security certificate. In most situations, the data subject has no idea a certificate exists or is being relied upon.

7.13. The concern that it would be difficult for an individual to appeal a certificate because any person "directly affected" by a certificate would not be notified of this fact, persists in the current Bill. It is unclear how the right to judicial review could be exercised without any way of knowing whether a national security certificate has been applied to their data. Even if a national security certificate was published, they are so broad as to be meaningless.

7.14. As noted by Deputy Counsel to the Joint Committee on Human Rights, 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 from considering the merits of the decision. The appeal rights of individuals are therefore restricted to a costly and narrow avenue of appeal.[17]

7.15. There are additional concerns.

7.16. In the current Bill, Chapter 3, which relates to the 'applied GDPR' as defined by the Bill contains two clauses dealing with national security. Clause **26** provides essentially that a controller is exempt from the vast majority of obligations and rights arising under the GDPR if exemption from the provision is required for the purpose of safeguarding national security or defence purposes. The provision includes most of the data protection principles and all of the rights granted to data subjects, as well as the Information Commissioner's enforcement powers[18].

7.17. Clauses 26 and 27 **do not relate to** law enforcement or intelligence agencies, but to 'general processing'. As noted by Deputy Counsel for the Joint Committee on Human Rights, 'It is not clear which organisations will be the beneficiaries of these certificates' under Part 2 of the Bill.

---

[17] §79 https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

[18] Deputy Counsel, Joint Human Rights Committee report §73 … 'Whether either 'national security' or 'defence purposes' are relied upon, exemptions apply to nearly all the data protection principles, all the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions.' https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

7.18. Clause 27 then permits Ministers of the Crown to issue certificates to the effect that the exemption applies. A Minister's certificate is 'conclusive evidence of [the] fact'[19] that the exemption is required for national security or defence purposes.

7.19. Clause **79**, Chapter 6, Part 3, makes similar provision for national security certificates to be issued in the context of law enforcement processing. Clause **111,** Chapter 6, Part 4, makes provision for national security certificates in the context of intelligence services processing.

7.20. However, the intelligence services are granted even more extensive exemptions, including exemptions from the oversight of the Information Commissioner. Clause **110** permits for national security certificates to exempt Schedule 13 (other general functions of the Commissioner), which includes provision for the Information Commissioner to monitor and enforce Parts 3 and 4 of this Bill. i.e. monitoring and enforcement can be exempted by a certificate. The effect of these exemptions is to allow Ministerial certificates to override the powers of the Information Commissioner.

7.21. Whilst certain exemptions may be required, it is unclear why the authorities require such a breadth of exemptions from their obligations under the data protection regime. As noted by Deputy Counsel, Joint Human Rights Committee 'Some of the data protection principles ought arguably to apply 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?'[20]

7.22. National security certificates are indefinite, they are timeless and retrospective - the Bill does not impose a time limit or a duty to review the ongoing necessity of the certificate.

7.23. It remains the case that there is no independent oversight or scrutiny of the issue of national security certificates.

---

[19] ibid §27(1)

[20] §75 https://www.parliament.uk/documents/joint-committees/human-rights/correspondence/2017-19/Note_Deputy_Counsel_DPBill.pdf

7.24. The object and purpose of the GDPR, the Law Enforcement Directive and in general the granting of data protection rights, is to enable individuals to have control over the processing of their personal data. The problem is, however, that certificates are often: (a) very broadly drawn; and (b) secret - they are not made public and/or not relied upon expressly by a controller in response to a data subject access request.

7.25. It is difficult for individuals or bodies to challenge secret certificates and/or the secret unconfirmed application of such certificates. Accordingly, the use of national security certificates not only operates to limit the scope of the appeal rights available to the individual - it also operates in a way which may (and often does) deny the data subject any knowledge of the existence of the certificate, as well as the processing of their data, thereby in practice negating their right of appeal. Thus, the lack of transparency and accountability surrounding the use of national security certificates gives rise to real questions as to whether data subjects are afforded effective judicial remedies for the enforcement of their rights.

7.26. The Data Protection Bill afforded the Government the opportunity to address these concerns arising out of the existing use of section 28 national security certificates.

7.27. As noted above, despite the fact that Schedule 13 envisages the Information Commissioner having a role supervising compliance with Parts 3 and 4 of the proposed Act, Clause 111 allows a certificate to oust the role of the Information Commissioner in large part.

7.28. Affording the Information Commissioner or Investigatory Powers Commissioner (whose role arising out of the Investigatory Powers Act 2016 explicitly deals with sensitive issues concerning national security) a clear and automatic role in supervising the issuing and enforcement of national security certificates would be an important step in ensuring the new Data Protection Act is applied lawfully.

7.29. It would be a step backwards to fail to include independent oversight of national security certificates.

7.30. The national security exemption regime not only undermines the right to privacy, it is likely to be a significant challenge to securing a

positive decision by the European Commission to grant adequacy to the UK post Brexit (see GDPR Article 45, 2(a)). In its current form the regime is deficient in basic principles of legality.

7.31. Deputy Counsel for the Joint Committee of Human RIghts has recommended consideration of 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. In addition to consider recommending the strengthening of oversight for the issuing of national security certificates, a further suggestion is to engage the Intelligence and Security Committee and the Independent Reviewer of Terrorism Legislation to explore these matters further.

7.32. We welcome these suggestions and encourage Members of Parliament to reflect on these urgent concerns.

8. Intelligence agencies - cross border transfers

8.1. The Bill provides for almost unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection.

8.2. Part 4 of the Bill covers the processing by the intelligence agencies (M15, MI6 and GCHQ). It is based on the Council of Europe modernised draft Convention 108 for the Protection of Individuals with Regard to the Processing of Personal Data.[21] Clause 109 of Part 4 provides for transfers of personal data outside the UK by the intelligence agencies.

8.3. Clause 109 does not provide an appropriate level of protection as required by Convention 108. Clause 109 of the Bill provides almost unfettered powers to intelligence agencies to transfer personal data outside of the UK. The only condition – namely 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 Services Act 1989 or Intelligence Services Act 1994 – **does not provide meaningful safeguards** as these purposes are significantly broad. As such this clause provides for no requirement of **appropriate level of protection** as demanded by Article 12 of "Convention 108" which this clause is said to implement.[22]

8.4. Clause 109 threatens human rights protections**.** Intelligence sharing arrangements between agencies in different countries 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. Non-transparent, unfettered and unaccountable intelligence sharing threatens the foundations of the human rights legal framework and the rule of law. In reviewing the UK's implementation of the International Covenant on Civil and Political Rights, the UN Human Rights Committee has specifically

[21] Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. (September 2016), available at: https://rm.coe.int/16806a616c

[22] Paragraph 43 of Explanatory Notes, Policy Background, Data Protection Bill [HL], available at: https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/17066en03.htm

noted the need to adhere to Article 17, "including the principles of legality, proportionality and necessity," as well as the need to put in "effective and independent oversight mechanisms over intelligence-sharing of personal data."[23]

8.5. The European Court of Human Rights has also expressed concerns regarding intelligence sharing and the need for greater regulation and oversight: "The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance … is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."[24] In the context of Privacy International's litigation on bulk data, where the legality of transfer and sharing of data by the intelligence agencies is the subject of court proceedings, it has emerged that there is little, if any, oversight and auditing in respect of the transfer of bulk data or remote access to it.

8.6. Clause 109 could impact on an adequacy decision for the UK. As part of leaving the EU, the UK will want to seek an adequacy decision from the EU Commission to enable transfers of personal data from the EU to the UK. An adequacy decision will take into account respect of human rights and fundamental freedoms and rules on the onward transfer of personal data.

8.7. The UK legal regime on intelligence sharing lacks the required minimum safeguards for human rights and clause 109 of the Bill as currently drafted fails to address this shortcoming and thereby fails to bring the data sharing regime into conformity with standards complying with human rights law.

Privacy International strongly recommends that Clause 109 is amended to:

- Specify that the transfer must be "provided by law"

[23] Concluding Observations on the Seventh Periodic Report of the UK, U.N. Human Rights Committee, U.N. Doc. CCPR/C/GBR/ CO/7, para. 24 (17 Aug. 2015).
[24] *Szabó and Vissy v. Hungary*, App. No. 37138/14, European Court of Human Rights, Judgment, para. 78 (12 Jan. 2016).

- Bring the transfer of personal data to third parties under Part 4 in line with provisions under Part 3 of the Bill (Law Enforcement). There is no rationale to justify transfers by intelligence agencies having lower safeguards than those applicable to law enforcement's transfer.