PRIVACY INTERNATIONAL

Briefing on the Data Protection Bill for Committee Stage in the House of Lords

Privacy International's briefing (General Processing)

27 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

Table of Contents

These proposed draft amendments and comments should be read in conjunction with PI's briefing on the Data Protection Bill for Second Reading in the House of Lords (http:/bit.ly/2zxLDZX**).**

1. Clarity and accessibility of structure

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.

The clarity of the Bill was raised by Peers who spoke in the second reading of the Bill on 10 October 2017. Lord Stevenson noted: "This is a tricky Bill to get hold of, first because of its size and volume." Baroness Ludford emphasised that the cross – referencing to the absent GDPR detracts from simplicity and coherence. Baroness Lane-Fox stated:

> "*I found this Bill incredibly hard to read and even harder to understand. I fear that we will not do enough to stop the notion, referred to by the noble Lord, Lord McNally, that we are sleepwalking into a dystopian future if we do not work hard to simplify the Bill and make it accessible to more people, the people to whom I feel sure the Government must want to give power in this updated legislation… Giving people rights is meaningful only if they know that they have them, what they mean, how to exercise them, what infringement looks like and how to seek redress for it.*"

The distinction between GDPR and 'applied GDPR' is unclear and not demonstrably necessary. There should not be a need to have two separate applications and those matters covered by the applied GDPR in Chapter 3 of Part 2 could also be covered by Chapter 2 of Part 2. This would mean that controllers, processors and data subjects would only need to grapple with Chapter 2 of Part 2 (read in conjunction with GDPR) when exercising their obligations and rights under the Bill and GDPR.

- We recommend incorporating the provisions of Chapter 3 of Part 2 into Chapter 2 of Part 2.

The exception to processing under Part 2 would be where the processing is covered by Parts 3 and 4 of the Bill. Insufficient explanation and justification has been provided as to the reasoning for separate regimes for data protection law for law enforcement (Part 3) and intelligence agencies (Part 4). This leaves room for confusion and erodes protections for data subjects in certain processing activities. These can be combined whilst ensuring effective implementation of the Law Enforcement Directive and the 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 data subjects) are applied.
- We also recommend that the Government produces a comprehensive explanation of the GDPR, with all the relevant derogation provisions of Chapter 2, Part 2, once this Act is passed - as a comprehensive translation for the public.

2. Delegated Powers

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

Clause 9: Special categories – remove ability to vary/ omit safeguards via regulations

Amendment

Page 6, line 1, leave out "varying or omitting conditions or"

Draft amended clause:

(6) The Secretary of State may by regulations –

(a) amend Schedule 1 by adding safeguards, and
(b) make consequential amendments of this section

Rationale

Article 9.1 of GDPR prohibits the processing of special categories of personal data, this is subject to limited exemptions set out in Article 9.2 of GDPR. These exemptions should be limited and subject to safeguards. We appreciate that unforeseen circumstances relating to the processing of special categories of personal data may arise which require the adding, varying or omission of conditions in the Bill. This could be a specific scenario where the processing is not covered by one of the existing conditions or where an existing condition is no longer necessary or is being used to justify processing which goes against the essence of data protection. Such scenarios should be limited and any such conditions should be necessary and proportionate and should be done by primary legislation, amending the Data Protection Act. The Secretary of State should not have the power to vary or omit safeguards in Schedule 1, but only add them.

Clause 15: Power to make further exemptions etc by regulations – remove wide ranging regulation making power

Amendment

Page 8, line 35, leave out clause 15 and at end insert -

"15A Power to make further exemptions etc by amendment to the 2017 Act

The powers in Article 6(3), 23(1), 85(2), and 89 of the GDPR to legislate on the legal basis for processing, restrictions to the scope of obligations and rights, processing carried out for journalistic purposes or the purpose of academic artistic or literary expression and process for archiving purposes, together with the respective safeguards set out in those Articles, are to be exercised by means of amendments of the 2017 Act."

Rationale:

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 as well as further restrictions on when the rights under GDPR apply. Future changes weakening the protections afforded by GDPR could impact on a future adequacy decision on the processing of personal data in the UK, therefore effective parliamentary scrutiny is essential.

Concerns about this regulation making power have been raised by academics[1] and Peers in the second reading of the Bill. Lord McNally stated that "*I do not believe that sprinkling Bills with Henry VIII clauses is an answer to the challenge of future-proofing*." Baroness Ludford stated that "*Very significant is the power for the Government under Clause 15 to confer exemptions from the GDPR by regulation rather than put them in primary legislation. That will need to be examined very carefully, not only for domestic reasons but also because it could undermine significantly an adequacy assessment in the future*." Lord Arbuthnot agreed with Baroness Ludford, stating that Clause 15 "*would allow the alteration of the application of the GDPR by regulations subject to affirmative resolution and that could include the amendment or repeal of any of the derogations contained in the Bill. I share the concern expressed by the noble Baroness, Lady Ludford, on that and we will need to look at it*." These concerns were also echoed by Baroness Jay of Paddington, who noted that she was "*concerned that the way some of the Bill is drafted already suggests that we are once again moving into that area where the role of this House and the other place is diminished by so much secondary legislation being proposed*."

For the above reasons, the proposed amendment seeks to ensure that any legislation under the provisions of Articles 6(3), 23(1), 85(2), and 89 of GDPR is only made by way of primary legislation with effective parliamentary scrutiny and are subject to the safeguards in each of these Articles.

Clause 169: Regulations and consultation – require public consultation re regulations

Amendments

Page 96, line 1, after Commissioner insert ", data subjects and persons who appear to the Commissioner to represent the interests of data subjects,"

Page 96, line 3, leave out paragraph (a)

---

[1] See 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/)

Draft amended clause:

(2) The Secretary of State must consult the Commissioner, data subjects and persons who appear to the Commissioner to represent the interests of data subjects, before making regulations under this Act, other than regulations made under –

(a) -
(b) section 28;
(c) etc..

Rationale

The wide regulation making powers under the Bill grant an unacceptable amount of power to the Secretary of State to introduce secondary legislation. The concerns regarding secondary legislation, including those voiced by Peers in the second reading of the Bill, are set out above.

Consultation is one way to seek to ensure oversight and scrutiny of regulations. As well as an obligation to consult the Commissioner, the Secretary of State should be under a statutory duty to consult data subjects and those who represent the interests of data subjects. Furthermore, the rationale for excluding section 21(Power to make provision in consequence of regulations related to the GDPR) from the duty to consult is not established and this exception should be removed from clause 169.

3. 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 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.

Clause 173: Representation of data subjects –add rights in Article 80.2 GDPR

Amendments

We support the proposed amendment by Lord Stevenson et al. and a further amendment drafted by Open Rights Group.

Page 98, line 20, at end insert—

"( )
In relation to the processing of personal data to which the GDPR applies, Article 80(2) of the GDPR (representation of data subjects) permits and this Act provides that a body or other organisation which meets the conditions set out in that Article has the right to lodge a complaint, or exercise the rights, independently of a data subject's mandate, under—

1. (a) Article 77(right to lodge a complaint with a supervisory body);
2. (b) Article 78 (right to an effective judicial remedy against a supervisory authority); and

3. (c) Article 79 (right to an effective judicial remedy against a controller or processor),

of the GDPR if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing."

Page 98, line 31, at end insert –

"() The rights in subsection (2)(a) - (d) may also be exercised by a body or other organisation that meets conditions in subsections (3) and (4) independently of a data subject's authorisation."

Rationale

These amendments would enable qualified NGOs to take up collective actions on behalf of consumers and citizens affected by data breaches and other illegal activities which may cause them financial or other detriment and of which they may not be aware to take action on their own. Such empowerment is provided for on an optional basis in GDPR (Article 80.2) and we are proposing that it is extended to cover the rest of the issues in the Data Protection Bill, since severe breaches of personal information frequently take place in the public sector. Such powers of collective redress are vitally important since personal data has become such an essential part of the national and global economy, while the imbalance of power and the information asymmetry makes it particularly difficult for individuals to claim their rights effectively. Furthermore, many breaches of data protection law affect thousands rather than single individuals, so collective redress actions are more efficient in such circumstances, as illustrated by many such successful actions carried out by NGOs in countries around Europe, based both on consumer protection and data protection legislation.

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

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.

Clarity re meaning of public interest and substantial public interest

Clause 7: Lawfulness of processing: public interest etc – limit condition

Amendment

Page 5, line 6, remove "includes" and insert "refers to"

Draft amended clause:

In Article 6(1) of the GDPR (lawfulness of processing), the reference in point (e) to processing of personal data that is necessary for the performance of a task carried

out in the public interest or in the exercise of the controller's official authority ~~includes~~ **refers to** processing of personal data that is necessary for—

(a) the administration of justice,

(b) the exercise of a function of either House of Parliament,

(c) the exercise of a function conferred on a person by an enactment, or

(d) the exercise of a function of the Crown, a Minister of the Crown or a government department.

Rationale

There is a lack of clarity around the meaning of the term 'public interest' in the Bill and GDPR. This is explained in more detail below. This lack of clarity is exacerbated by clause 7 of the Bill, which includes a non-exhaustive definition of processing that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority. This clause also detracts from the safeguards provided in Article 6(2) and (3) of GDPR. Article 6(2) provides that whilst a Member State may maintain or introduce more specific provisions with regard to processing for compliance with part (e) this should be done to determine more precisely specific requirements for the processing and other measures to ensure lawful and fair processing . Article 6(3) provides that the basis for processing in point (e) must be laid down by law, and that the specific provisions should include measures to ensure fair and lawful processing. Furthermore, the law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Clause 7 should therefore be amended to make the list of activities which fall within point (e) specific and exhaustive.

Add a requirement to publish code of practice/ guidance re public interest

Amendment

Page 66, line 2, at end insert:

"120A Public interest code

(1) The Commissioner must prepare a code of practice which contains –
(a) Practical guidance in relation to the processing of personal data in the public interest
(b) Practical guidance in relation to the processing of personal data in the substantial public interest
(c) Such other guidance as the Commissioner considers appropriate to promote an understanding of the application of the terms public interest and substantial public interest in the context of the 2017 Act.

(2) Where a code under this section is in force, the Commissioner may prepare amendments of the code or a replacement code.

(3) Before preparing a code or amendments under this section, the Commissioner must consult the Secretary of State and –
(a) Data subjects
(b) Persons who appear to the Commissioner to represent the interests of data subjects.

(4) A code under this section may include transitional provision or savings.

(5) In this section –
"public interest" means public interest as used in the 2017 Act and the GDPR
"substantial public interest" means substantial public interest as used in the 2017 Act and the GDPR

N.B Consequential amendments would be needed to s121 – 123 to include reference to Code published under 120A

Rationale

The term 'public interest' is used throughout the Data Protection Bill and is key to applying many of its provisions. These include consideration of the legal basis/ condition for processing, whether an exemption applies, whether the data can be transferred and as a defence to certain offences. In relation to special categories of personal data, the term 'substantial public interest' is used in the Bill (as in GDPR). Neither 'public interest' or 'substantial public interest' are defined terms in the Bill.

Concerns regarding the lack of clarity around the term 'public interest' and 'substantial public interest' were raised during the second reading of the Bill in the House of Lords. Baroness Ludford stated: "*We may need seriously to look at the lack of definition of "substantial public interest"* as a basis for processing sensitive data, or even of public interest." and Lord Patel raised the issue in the context of research.

The below table sets out the many provisions of the Bill which require consideration of the 'public interest' or 'substantial public interest:

Clause	
7	**Lawfulness of processing in the public interest** (non-exhaustive definition of what is included within Article 6(1)(e) of GDPR
15	**Power to make further exemptions etc by regulations** broad power for Government to amend GDPR by way of Regulations

17	**Transfers of personal data to third countries etc** where there are important reasons of public interest
39 & 85	**Archiving** applies where archiving purposes are in the public interest
74 & 75	**Transfers** requires consideration of the rights of the data subjects and the public interest in the transfer
127	**Confidentiality of information** disclosures in the public interest
162	**Re-identification of personal data** public interest defence
171	**Prohibition of requirement to produce relevant records** public interest defence
173	**Representation of data subjects** Representative body must have objectives in the public interest
Sch 1 Part 1 para 3 para 4 Sch 1 Part 2 Para 6 Para 8 Para 9 Para 10 Para 13	**Condition for processing special categories** Public interest in public health Archiving/ research in public interest **Requirement of substantial public interest*** Parliamentary, statutory and government purposes Preventing or detecting unlawful acts Protecting the public against dishonesty Journalism + publication in the public interest Counselling
Sch 2 para 7 para 24 para 26	**Exemptions from GDPR** Functions of a public nature exercised in the public interest Publication in the public interest Archiving in the public interest

Further clarification on the scope of "public interest" and "substantial public interest" in the Bill is required. Guidance is needed on how these terms are to be interpreted when applying the provisions of the Bill. The application of a public interest test or substantial public interest test, will to an extent be dependent on the particular circumstances of the processing. However, guidance on the application of these terms from the ICO would provide clarity and greatly assist controllers and processors in carrying out their obligations and data subjects in understanding whether their data is being processed in accordance with the terms of the legislation. Guidance would be in important to tool to prevent misapplication/ interpretation of these terms which could lead to individuals' personal data being processed without a valid legal basis or being incorrectly subject to an exemption.

Under the current Bill it is at the discretion of the ICO as to whether to publish guidance or a code of practice on the public interest. No such guidance has been published to date, despite the use of both public interest and substantial public interest in the Data Protection Act 1998 and associated statutory instruments. Given the increased importance of these terms under the GDPR and the Bill (which aims to strengthen the rights of data subjects and imposes higher penalties on controllers and processors for breaches as well as further individual offences), it is critical to the consistent application of the terms of the Bill (and GDPR) that guidance on the public interest is available and that controllers and processors take this guidance into account when interpreting and applying the relevant provisions of the Bill/ GDPR.

The desired form of guidance would be a statutory Code of Practice which would require the Commissioner to produce such guidance and allow for it to be consulted upon and scrutinised by Parliament. Whilst failure to act in accordance with the Code would not in itself make a person liable to legal proceedings it could be taken into account by a Court or the Commissioner when considering proceeding or regulatory action and there would therefore be a strong incentive for controller's and/or processors to take into account and comply with the Code.

By way of background and for reference, 'public interest' is an issue which is also relevant to freedom of information and guidance is available as to its application in this context.

Public interest in Freedom of Information

Freedom of information legislation in the UK (the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002) requires the application of a 'public interest test' in relation to certain exemptions to right of freedom of information. Even where certain exemptions apply, there is then a requirement to go on and consider the public interest in withholding the information versus the public interest in disclosing the information, with the presumption being in favour of disclosure. Both the ICO (responsible for FOI in England and Wales) and the Scottish Information Commissioner (responsible for FOI in Scotland) have published detailed guidance on the application of this test[2]. This guidance is relied upon by public authorities in the practical application of exemptions under the legislation.

Conditions for processing special categories of personal data in the substantial public interest (Sch 1 Part 2)

Remove specific condition regarding political parties

[2] ICO – The public interest test https://ico.org.uk/media/for-organisations/documents/1183/the_public_interest_test.pdf
Scottish Information Commissioner - The public interest in FOISA
http://www.itspublicknowledge.info/Law/FOISA-EIRsGuidance/ThePublicInterestTest/thePublicInterestTestFOISA.aspx

Part 2 of Schedule 1 to the Bill, sets out the conditions for processing special categories of personal data based on Article 9(2)(g) of GDPR which provides that:

> *"processing is necessary for **reasons of substantial public interest**, on the basis of Union or Member State law which shall be **proportionate to the aim pursued**, **respect the essence of the right to data protection** and **provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject**;"*

Neither the Bill nor the explanatory notes explain how the conditions in Part 2 of Schedule 1 meet the requirements of Article (9)(2)(g).

Paragraph 17 – Political parties

Of particular concern is paragraph 17 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. This can include, but is not restricted to, campaigning, fundraising, political surveys and case-work. Whilst a variation of this condition was included in a statutory instrument 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).

Developments in profiling practices and concerns

Using voter personal information for campaigning is nothing new. For decades political parties have been using and refining targeting, looking at past voting histories, religious affiliation, demographics, magazine subscriptions, and buying habits to understand which issues and values are driving which voters. However, what is new and has been enabled by technologies is the granularity of data available for such campaigning, to the extent that political campaigners have come to know individuals' deepest secrets. This is well documented in the US for example, where the Republican National Committee provides all Republican candidates with free access to a database that includes data on 200 million voters and includes over 7 trillion micro targeting data points. Political campaigners have moved towards knowing individuals' deepest secrets through gathering thousands of pieces of scattered information about them. Sensitive information, such as political beliefs, can be revealed from completely unrelated data using profiling. The fact that commercial data, public records, and all sorts of derived information, or Facebook likes, are used for political campaigning would come as a surprise to most people.

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[3] . However, unlike party-political broadcasts on TV, 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 or the media. 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[4].

A fundamental reason why in a democracy (unlike in the recent party Congress voting in China!) ballots are secret, is to forestall attempts to influence voters by any form of intimidation, blackmailing, or lies. Through granular profiling, political parties can obtain the political preferences and likely past voting decisions of millions of voters. This is a dangerous development for democracy going forward.

Position under the Data Protection Act 1998 (DPA)

A variation of this condition in paragraph 17, was included in the Data Protection (Processing of Sensitive Personal Data) Order 2000 made under Schedule 3 to the DPA. Paragraph 8 of the 2000 Order permitted registered political parties to process information **consisting** of an individual's political opinions, in the course of their political activities, where this does not cause nor is likely to cause substantial damage or substantial distress to them or any other person and where they have not served notice requiring the party to cease the processing.

Why paragraph17 re political parties should be removed

There are a number of reasons as to why this condition should be removed from the Data Protection Bill:

1) Consistency with the DPA is not a justification for including a condition for processing in the Bill. The DPA is not a gold standard of data protection and many of its provisions have not received sufficient scrutiny regarding their impact on privacy, in the almost 20 years since the legislation was enacted.

2) Paragraph 17 has not been copied explicitly from the DPA, there is a subtle but important change in wording, which widens the scope to personal data ***revealing*** political opinions.

---

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

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*

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

3) Developments in technology enable political parties to process personal data in a manner and on a scale, that was not possible when the DPA was enacted. Concerns with these practices (profiling) and their implications for the democratic political process, together with the lack of public scrutiny are set out above.

4) The broad condition in paragraph 17, goes beyond what is set out in recital 56 of GDPR which provides that "Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are in place." Neither the wording of the condition in paragraph 17 nor the explanatory notes explain why the operation of a democratic system in the UK **requires** that political parties compile personal data on people's political opinions. The word 'revealing' and the non-defined broad scope of 'political activities, in paragraph 17, together with the threshold of 'substantial damage or substantial distress', go beyond processing that required for electoral activities in a democratic system.

5) There are already sufficient conditions for processing in the GDPR and the Bill, that political parties can rely on for processing personal data of individuals. If the processing involves non-personal data, such as names and contact details then parties can seek to rely on consent (Art 6.1(a) of GDPR) or legitimate interests (Art 6.1(f)) of GDPR). If it is political opinions of individuals, then the GDPR provides alternate conditions, including explicit consent (Art 9.2 (a) of GDPR) or processing is of the political opinions of members/ former members or those in regular contact with the party, and carried out in the course of the party's legitimate activities, with appropriate safeguards (Art 9.2(d) of GDPR).

6) The condition in paragraph 17(1) of Schedule 1to the Bill, does not meet the requirements of Article 9(2) derogation of GDPR. The condition is not demonstrably in the substantial public interest and it is not proportionate. This condition would legitimize and give a legal basis to, the practices described above, involving the granular scrutiny of personal data that for the concerns set out above is not in the substantial public interest. Political parties should rely on other conditions, such as explicit consent, before processing personal data revealing political opinions. The onus should be on political parties to explain in clear terms, to the public, how they process personal data revealing political opinions and why this condition is necessary. Only with transparency around the current and envisaged processing of political opinions by political parties, can a thorough proportionality and impact assessment be carried out around this condition.

For the reasons identified above, there are significant concerns as to the prejudice to the fundamental rights and interests of individuals caused by processing under this condition. No justification has been provided as to the legitimate aim pursued and on this basis the condition should be removed from the Bill.

Ways in which paragraph 17 re political parties could be improved

Privacy International's position is that paragraph 17 should be removed from the Bill for the reasons set out above. However, on the basis that explanation and justification are provided by Government and political parties to demonstrate the legitimate aim that this condition pursues, then amendments must be made to seek to ensure that the scope of the condition is proportionate and adequate safeguards are established. The details of such amendments are for Parliament to decide, however suggested amendments are:

1) that the word 'revealing' is removed;

2) that 'political activities' is exhaustively defined and limited in scope;

3) that 'substantial' is removed from the threshold in paragraph 17(2) and processing under this condition (paragraph 17(1)) should be prohibited where it is likely to cause damage or distress;

4) that at the point of informing data subjects of the processing in accordance with Articles 13 or 14 of GDPR, political parties clearly inform individuals of their right to opt-out (paragraph 17(3) and make this right easy to exercise.

5. Automated decision making authorised by law: safeguards

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.

Clause 13: Automated decision-making authorised by law

Amendments are suggested in order to:

1. Clarify the meaning of decision "based solely on automated processing";
2. Strengthen safeguards regarding automated decision-making authorised by law;
3. Ensure full right to challenge and redress regarding automated decision-making authorised by law

<u>Amendments</u>

Clause 13: clarify the meaning of decision "based solely on automated processing"

Page 7, line 11, at end insert:

"( ) A decision is 'based solely on automated processing' for the purposes of this section if, in relation to a data subject, there is no meaningful input by a natural person in the decision-making process."

Clause 13: Strengthen safeguards regarding automated decision-making authorised by law

Page 7, line 26 at end, after "and" insert:

"provide meaningful information about the logic involved as well as the significance and legal consequences of such processing; and"

Clause 13: Ensure full right to challenge and redress regarding automated decision-making authorised by law

Page 7, line 39, after paragraph (5), insert:

"( ) Data subject affected by a qualifying significant decision under this section retains the right to lodge a complaint to the Commissioner under Clause 156 and to seek compliance order by a court under Clause 158."

Rationale

Automated decision-making and profiling

Our world is one in which more and more of what we do is traceable, where aggregated data can reveal a lot about a person and where we see ever increasingly sophisticated means of processing data with regards to automated decision-making.

The profiling of individuals can inform automated decision-making and therefore cannot be isolated from considerations around automated decision-making: profiling itself can automate inferences and predictions by relying on an expanding pool of data sources, such as data about behaviour, location and contacts, as well as increasingly advanced data processing, such as machine learning.

To ensure data protection legislation can address the technological challenges that exist now and that lie ahead, we must ensure that profiling and automated decisions it informs are legal, fair and not discriminatory, and that data subjects can exercise their rights effectively.

Profiling, which may be relied upon to make automated decisions, refers to a form of programmed processing of data, using algorithms, to derive, infer, predict or evaluate certain attributes, demographic information, behaviour or even the identity of a person. Profiling can involve the creation, discovering or construction of knowledge from large sets of data. In turn created profiles can be used to make decisions.

When considering the input that may be used in decision-making, profiling can infer or predict highly sensitive details from seemingly uninteresting data, leading to detailed and comprehensive profiles that may or may not be accurate or fair.

The reliance on computational algorithms and machine learning (see Annex C for more details and examples), may pose a number of challenges, including with regards to

opacity and auditability of the processing of data. One way to tackle this is to strengthen safeguards regarding automated decision-making authorised by law.

When is automated decision-making harmful?

Automated decision-making, informed by profiling practices, is widespread and central to the way we experience products and services: recommender systems rely on fine-grained profiles of what we might next want to read, watch, or listen to; dating apps rank possible partners according to our predicted mutual interest in each other; social media feeds are automatically personalised to match our presumed interest; and online ads are targeted to show what we might want to buy at a time when we are most likely to be perceptive.

At the same time, however, it poses three closely related risks:

- By virtue of generating new or unknown information, it is often highly privacy invasive.

- It challenges common views about consent and purpose limitation, and also raises issues around control, not just over personal data, but also one's identity. Data subjects may be unaware of the kinds of inferences and predictions that can be revealed[5] and used in automated decision-making.

- Since derived, inferred or predicted profiles may be inaccurate, or otherwise systematically biased, profiling may also lead to individuals being misclassified or misjudged. When profiling is used to inform or feed into automated decisions that affect individuals, the outcome of such decisions may result in harm – regardless of whether this decision is fully automated or not. In the words of the UN Human Rights Council,

  "*automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights.*"[6]

There is a risk that this can be used to the detriment of those who are already discriminated and marginalised. Even if data controllers can take measures to avoid processing sensitive data in automated processing, trivial information can have similar results to sensitive data being processed.[28] In racially segregated cities, for instance, postcodes may be a proxy for race. Without explicitly identifying a data subject's race, profiling may therefore nonetheless identify attributes, or other information that would nonetheless lead to discriminatory outcomes, if they were to be used to inform or make a decision.

[5] The Royal Society, 2017, Machine learning: the power and promise of computers that learn by example. *Royal Society*. Available from https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf [Accessed 1st August 2017]
[6] U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1 (22 March 2017)

In this context, the Bill is an opportunity to ensure rights are protected and safeguards exists.

Clarify the meaning of decision "based solely on automated processing"

Automated decision rights are able to be triggered for decisions with *legal effects or similarly significant effect*, but only if these decisions are *based solely* on automated processing. If decisions involve a "human-in-the-loop" they can avoid decisions being subject to the safeguards, even if the human is just agreeing with the system.

Proprietary software, such as the COMPAS risk assessment that was sanctioned by the Wisconsin Supreme Court in 2016[7], calculates a score predicting the likelihood of committing a future crime. Even if final decisions are made by a judge, the software's automated decisions can be decisive, especially if judges rely on them exclusively or haven't been warned about their risks, including that the software produced inaccurate, illegal, discriminatory or unfair decisions.

This is particularly concerning in the context of automation bias, i.e. the propensity for humans to favour suggestions from automated systems over contradictory information made without automation, even if correct.[8] As a result, decisions that are formally attributed to humans but are *de facto* determined by an automated data-processing operation should clearly fall within the applicability of the provision.

As a matter of fact, all systems that exercise automated processing or decision-making are designed, operated and maintained by humans, whose involvement inevitably influences the outcomes and decisions made. Furthermore, human influence is embedded into software. The outcomes and decisions made by algorithms, for instance, are shaped by human decisions about training data (i.e. what data to feed the computer to 'train' it), semantics, criteria choices etc. For Clause 13 to be applicable, "solely" cannot exclude any form of human involvement.

We recommend defining decisions as "solely" based on automated processing where there is no "meaningful human input".

As noted in the recently published draft guidelines on profiling by the Working Party 29 (i.e. the body representing all national data protection authorities in the EU, including the ICO which led on the consultation of this document), the:

> "*controller cannot avoid the Article 22 provisions by fabricating human involvement. For example, if someone routinely applies automatically generated profiles to individuals without any actual influence on the result, this would still be a decision based solely on automated processing. To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather*

[7] Citron, D., 2016, (Un)Fairness of Risk Scores in Criminal Sentencing. *Forbes*. Available from: https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal-sentencing/#6074794b4ad2. [Accessed 1st August 2017]

[8] See for instance Skitka, L.J., Mosier, K.L. and Burdick, M., 1999. Does automation bias decision-making?. *International Journal of Human-Computer Studies*, *51*(5), pp.991-1006.

than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the available input and output data." [9]

For the purposes of clarity of obligations imposed on controllers, it is important that this explanation is included in the Bill.

We note the suggestion of the ICO, issued in a Feedback request on profiling and automated decision-making, that an effect is already significant if it has "*some consequence that is more than trivial and potentially has an unfavourable outcome*".[10]

Strengthen safeguards regarding automated decision-making authorised by law

The provision of meaningful information about the logic involved as well as the significance and legal consequences of such processing is fundamental to allow transparency of automated decision making and ensure accountability and the rights of data subjects, including having sufficient information in order to challenge such decisions. There is no rationale for omitting it in this section.

This amendment to ensure a right to explanation is an automated-decision safeguard, in line with the Government's own Explanatory Notes (para 115)[11] and Recital 71 of the EU GDPR:

"*The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.*

Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

However, decision-making based on such processing, including profiling, should be allowed where expressly authorized by Union or Member State law to which the

[9] http://ec.europa.eu/newsroom/document.cfm?doc_id=47742

[10] Information Commissioner's Office, 2017. Feedback request – profiling and automated decision-making. *ICO.* Available from https://ico.org.uk/about-the-ico/consultations/feedback-request-profiling-and-automated-decision-making/

[11] 115. The GDPR does not set out what suitable safeguards are, though recital 71 suggests they should include:

- provision of specific information to the data subject; and
- right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after an assessment, and an opportunity to challenge the decision.

controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent.

In any case, such processing should be subject to ***suitable safeguards****, which should include* ***specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision"****.*

The obligation to provide information about the logic involved in the automated decision is already contained in the GDPR (Article 13(2)(f), Article 14(2)(g) and Article 15(1)(h).) Such provisions are also essential in the case of automated decision-making authorised by law.

It has been suggested that subject access rights as per Article 15 (1) (h) of the GDPR are sufficient. This is not however the case, as that Article specifically refers to the right to have the information regarding automated-decision making, including profiling and the logic involved referred to in Article 22(1) and (4); **therefore Article 22 (b) which exempts automated decision-making authorised by Member State law is not included in this provision**. To ensure effective safeguards as suggested by Recital 71 of GDPR, the protection must be in Clause 13 itself, to provide for meaningful information about the logic involved as well as the significance and legal consequences of such processing.

Provision of meaningful information may be a step towards addressing concerns about the extent to which automated decisions rely on data that has been derived or predicted through profiling. Whilst not within the scope of the proposed amendment, guidance could require information to include:

- What data will be used as input;
- What categories of information data controllers intend to derive or predict;
- How regularly input data is updated;
- Whether the actions of others affect how data subjects are profiled;
- The presence of algorithms;
- What kinds of measures the data controller will take to address and eliminate bias, inaccuracies and discrimination. Since misidentification, misclassification and misjudgement are an inevitable risk associated to profiling, controllers should also notify the data subject about these risks and their right to access and rectification.

Ensure full right to redress

Automated decision making, including profiling, affects data subjects in a variety of ways. The potential harms caused by profiling have been confirmed by the United

Nations Human Rights Council, which noted with concern "that automatic 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". Given this potential negative impact, data subjects must be expressly given the right to challenge automated decisions, when done in accordance with this section.

Article 22(2)(b) of the GDPR requires member states to establish "suitable measures to safeguard the data subject's rights and freedom and legitimate interest". Article 23 (3), and related recital 71 (see above), further requires the data controller to *"…implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*"

A right to effective remedy is definitely among the fundamental safeguards required: this is a separate right to redress than the remedies in the GDPR and the Enforcement section of the Bill, which only cover an infringement of the data subject rights as set out in the legislation. So the Bill needs to specifically refer to a right to challenge and redress in cases, for example, where a decision is discriminatory with consequences that prejudice the rights and freedoms of the data subject.

Further, guidelines should be provided on adequate forms of redress for irregularities that come to light as a result of the exercise of these rights, in particular with regards to "meaningful information" "logic of processing" and "envisaged consequences".

6. National Security Certificates (Part 2, Clauses 24, 25 and 26)

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 recommend a number of concrete obligations to be included in the Bill.

Introduction

These amendments focus solely on Clauses 24, 25 and 26 in Part 2. For ease of reference a full track changed edit of these clauses is set out at Annex A at the end of this document.

It is unclear at the outset who these provisions would apply to given:

(a) They do not relate to Law Enforcement processing (Part 3 of the Bill and Schedule 7)
(b) They do not relate to Intelligence Services processing (Part 4 of the Bill)
(c) They are in Part 2 being the 'applied GDPR' however, we are unsure what processing is outside the scope of EU law and therefore would fall within Part 2 and thus be affected by these clauses.

The lack of transparency around certificates, the absence of Parliamentary scrutiny and lack of public review into this regime, since the Data Protection Act 1998 came into force, results in a near total lack of awareness as to what certificates currently exist. It is thus impossible to deduce what entities may benefit in the future from exemption from GDPR and the Data Protection Bill as set out in Clauses 24, 25 and 26.

It is of concern that this in turn makes the necessity, proportionality and risk posed by these provision hard to evaluate.

We note that in their current form, certificates are timeless in nature, lack transparency, are near impossible to challenge and offer overly broad exemptions from data protection principles.

Clause 24: national security and defence exemption

Amendment

A full draft of the proposed amendment to Clause 24 is set out at Annex A. We submit the entire Clause 24 should be deleted.

Page 14, line 35 to page 15, line 32, leave out clause 24

Rationale

This clause should be deleted and instead Clause 25 modified as set out below to ensure a transparent process accompanied by safeguards to permit a route to seek exemption from aspects of the Bill for national security purposes. This must be accompanied by a mechanism for oversight.

We are concerned that included in the exemptions (page 15, line 33, (i) is section 173 of the Data Protection Bill 'representation of data subjects', which appears to undermine access to justice for those seeking to challenge a certificate.

In addition, this clause introduces a new defence purposes exemption (reflected also in Clause 25) which is an expansion on the Data Protection Act 1998 national security exemption in section 28. It is not explained, defined or elaborated as to what the purpose of this addition is and what it covers.

A full list of what this clause exempts is set out at Annex B below. This visibly demonstrates the unjustified breadth of this exemption.

The national security exemption has the potential to undermine a decision by the European Commission to grant adequacy to the UK post Brexit (see GDPR Article 45, 2(a)), particularly in its current form and in light of this regime which is lacking in basic safeguards, transparency and oversight.

Clause 25: National security: certificate

A track changed version of proposed amendments to Clause 25 is set out in Annex A at the end of this document.

Amendments

Page 15, line 34, delete "Subject to subsection (3), a certificate signed by"
Page 15, line 35, insert after "a Minister of the Crown" the words "must apply to a Judicial Commissioner for a certificate, if exemptions are sought"
Page 15, line 35, delete "certifying that exemption"
Page 15, line 35, insert after "from" the word "specified"
Page 15, line 35, delete the words "all or any of the"
Page 15, line 35 – 36 delete the words "listed in section 24(2) is, or at any time was, required"
Page 15, line 37, delete the words "conclusive evidence of that fact"

Page 15, line 37, insert new subsections:

(2) The decision to issue the certificate must be:

a. approved by a Judicial Commissioner,
b. laid before Parliament,
c. published and publicly accessible on the Cabinet Office website.

(3) In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Minister's conclusions as to the following matters:

a. Whether the certificate is necessary on relevant grounds, and
b. Whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and
c. Whether it is necessary and proportionate to exempt all provisions specified in the certificate.

Page 15, line 38, insert before "A certificate" the words "An application for"
Page 15, line 39, delete the word "may"
Page 15, line 39, insert before the word "identify", the word "Must"
Page 15, line 39, delete the word "general"
Page 15, line 39, insert after the words "means of a" the word "detailed"
Page 15, line 41, insert new subsections in clause 24(2) which states:

a. …
b. **Must specify each provision of this Act which it seeks to exempt, and**
c. **Must provide a justification for both (a) and (b).**
d. **…**

Page 15, line 41, delete the subsection (2(b)) which states "may be expressed as having prospective effect."

Page 15, after line 41, insert new subsections which state:

Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Judicial

Commissioner must give the Minister of the Crown reasons in writing for the refusal.

Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Minister may apply to the Information Commissioner for a review of the decision.

It is not permissible for exemptions to be specified in relation to:

a. Chapter II of the applied GDPR (principles) –
   i. Article 5 (lawful, fair and transparent processing)
   ii. Article 6 (lawfulness of processing)
   iii. Article 9 (processing of special categories of personal data)
b. Chapter IV of the applied GDPR –
   iv. Articles 24 – 32 inclusive;
   v. Articles 35 – 43 inclusive;
c. Chapter VII of the applied GDPR (remedies, liabilities and penalties)
   vi. Article 83 (general conditions for imposing administrative fines);
   vii. Article 84 (penalties);
d. Part 5 of this Act –
   viii. Section 112;
   ix. Section 113 (general functions of the Commissioner), subsections (3) and (8);
   x. Sections 114 – 117;
e. Part 7 of this act, section 173 (representation of data subjects)

Page 15, line 42, insert after the words "Any person" the words "who believes they are"
Page 15, line 42, insert after the word "directly" the words "or are indirectly"
Page 15, line 43, insert after the words "against the certificate" the word ", and"
Page 15, line 43, insert subjection which states "rely upon section 173 of this Act"

(1) Any person **who believes they are** directly **or are indirectly** affected by a certificate under subsection (1)
   a. may appeal to the Tribunal against the certificate, and
   b. rely upon section 173 of this Act.

Page 15, lines 44 – 45, delete the words "applying the principles applied by a court on an application for judicial review"
Page 15, line 45, insert after the words "judicial review" the words "it was not necessary or proportionate to issue"
Page 15, lines 45 – 46, delete the words "the Minister did not have reasonable grounds for issuing"

Page 16, lines 1 – 20, delete clauses (5), (6), (7), (8), (9).

Rationale

The national security exemption provisions contained in Part 2 Chapter 3 ('applied GDPR') to a large extent mirrors the extremely wide exemption from the Data

Protection Act 1998 where a national security certificate has been made. The provision allows exemption from all rights of the data subject.

National security certificates have never been subject to any oversight, review, critique by Parliament or any other statutory body. Certificates are timeless in nature and there is no transparency in relation to this regime. The Data Protection Bill presents an opportune moment to reform this opaque and undemocratic regime.

It is unacceptable that a certificate exemption from provisions of the GDPR and/or Data Protection Bill is granted to unknown entities, potentially private security firms, which do not fall within Part 3 Law Enforcement processing and Part 4 Intelligence Agencies processing. Particularly where there are no provisions for fundamental safeguards. It is unacceptable that the word of the Minister, particularly when there is not even basic oversight, is 'conclusive evidence'.

Any certificate must be ordered by the Judicial Commissioner, rather than the Minister simply signing it through. Rather than ministerial sign off, the minister should apply for an order exempting the particular processing from specific provisions.

A fundamental and basic safeguard is to introduce a procedure for a Minister of the Crown to apply to a Judicial Commissioner for a certificate who must review the Minister's conclusions as to necessity and proportionality. To ensure oversight and safeguards are effective, sufficient detail is required in the certificate application.

It may be necessary to make further provisions to provide for involvement for a Judicial Commissioner. We leave this to Parliament to consider and note that an oversight role can be performed by the Investigatory Powers Commissioner.

To address the current opaque nature of national security certificate we propose that all certificates are laid before Parliament and publicly accessible. We encourage Parliament to publish all current and extant certificates.

We have set out in a new clause, aspects of the GDPR and Data Protection Bill which can never be exempted. This mirrors the provisions in clause 24 which are not permitted to be exempted by way of a national security certificate.

We believe that Parliament must debate which aspects of the Data Protection Bill should never be exempted in this Chapter as the list we have identified is the bare minimum.

In addition to those aspects of GDPR and this Bill which should never be exempt, as referred to above, we have added clause 173 which we believe should never be exempted by a national security certificate.

The right to challenge a certificate has been modified to include those who believe they are directly or indirectly affected. Given the highly secretive nature of certificates it is logical to include these amendments.

Clause 26 National Security and defence: modifications to Articles 9 and 32 of the applied GDPR

Amendments

page 16, line 25, delete the words 'and defence'

page 16, line 30 - 31, delete the words 'or for defence purposes'

page 16, delete subsections (2) (3) (4).

Rationale

The Bill expands national security exemption to provide for a 'defence' exemption in the 'applied GDPR'. No definition has been provided nor clarification in the explanatory notes as to what it covers.

There is no justification for exempting Article 32 GDPR (security of processing)

7. Other - Exemptions (Schedule 2)

Remove immigration exemption

Amendment:

Page 125, line 40, leave out paragraph 4

Rationale:

The immigration exemption is new in the Bill and there was no direct equivalent under the Data Protection Act 1998. This is a broad and wide ranging exemption which is open to abuse. This exemption should be removed all together 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. Concerns about this exemption have been raised by other commentators and we support other civil society organisations who are also pushing for the removal of this exemption.[12]

[12] See Amberhawk blog 09/10/2017 http://amberhawk.typepad.com/amberhawk/2017/10/dp-bills-new-immigration-exemption-can-put-eu-citizens-seeking-a-right-to-remain-at-considerable-dis.html

Annex A: full track-change edit of clauses 24, 25, 26

Clause 24: National security and defence exemption

~~(1) A provision of the applied GDPR or the Act mentioned in subsection (2) does not apply to personal data to which this Chapter applies, subject to subsection (2) if exemption from the provision is required for –~~

~~a. The purpose of safeguarding national security, or~~

~~b. Defence purposes~~

~~(2) Provisions~~

~~(3) The provisions are –~~

~~a. Chapter II of the applied GDPR (principles) except for –~~

~~i. Article 5(1)(a) (lawful, fair and transparent processing) so far as it requires processing of personal data to be lawful;~~

~~ii. Article 6 (lawfulness of processing);~~

~~iii. Article 9 (processing of social categories of personal data);~~

~~b. Chapter III of the applied GDPR (rights of data subjects);~~

~~c. In Chapter IV of the applied GDPR~~

~~i. Article 33 (notification of personal data breach to the Commissioner);~~

~~ii. Article 34 (communication of personal data breach to the data subject);~~

~~d. Chapter V of the applied GDPR (transfers of personal data to third countries or international organisations)~~

~~e. In Chapter VI of the applied GDPR –~~

~~i. Article 57(1)(a) and (h) (Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations (;~~

~~ii. Article 58 (investigative, corrective, authorisation and advisory powers of Commissioner);~~

~~f. Chapter VIII of the applied GDPR (remedies, liabilities and penalties) except for –~~

~~i. Article 83 (general conditions for imposing administrative fines);~~

~~ii. Article 84 (penalties);~~

~~g. In Part 5 of this Act –~~

~~i. In section 113 (general functions of the Commissioner) subsections (3) and (8);~~

~~ii. In section 113, subsection (9), so far as it relates to Article 58(2)(i) of the applied GDPR;~~

~~iii. Section 117 (inspection in accordance with international obligations);~~

~~h. In Part 6 of this Act –~~

~~i. Sections 137 to 147 and Schedule 15 (Commissioner's notices and powers of entry and inspection);~~

~~ii. Sections 161 to 163 (offences relating to personal data);~~

~~i. In Part 7 of this Act, section 173 (representation of data subjects).~~

Clause 25: National security : certificate

(1) ~~Subject to subsections **(2) and** (3),~~ ~~a certificate signed by~~ **A** Minister of the Crown **must apply to a Judicial Commissioner for a certificate, if exemptions are sought** ~~certifying that exemption~~ from **specified** ~~all or any of the~~ provisions **of this Act** ~~listed in section 24(2) is, or at any time was, required~~ in relation to any personal data**,** for the purpose of safeguarding national security is ~~conclusive evidence of that fact.~~

(2) The decision to issue the certificate must be:

- **a. approved by a Judicial Commissioner,**
- **b. laid before Parliament,**
- **c. published and publicly accessible on the Cabinet Office website.**

(3) In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Minister's conclusions as to the following matters:

- **a. Whether the certificate is necessary on relevant grounds, and**
- **b. Whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and**
- **c. Whether it is necessary and proportionate to exempt all provisions specified in the certificate.**

(4) **An application for** a certificate under ~~subsection (1)~~**:**

- a. **Must** ~~may~~ Identify the personal data to which it applies by means of a ~~general~~ **detailed** description, and
- b. **Must specify each provision of this Act which it seeks to exempt, and**
- c. **Must provide a justification for both (a) and (b).**
- d. ~~May be expressed to have prospective effect~~.

(5) **Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.**

(6) **Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Minister may apply to the Information Commissioner for a review of the decision.**

(7) It is not permissible for exemptions to be specified in relation to:

- a. Chapter II of the applied GDPR (principles) –
  - i. Article 5 (lawful, fair and transparent processing)
  - ii. Article 6 (lawfulness of processing)
  - iii. Article 9 (processing of special categories of personal data)
- b. Chapter IV of the applied GDPR –
  - i. Articles 24 – 32 inclusive;
  - ii. Articles 35 – 43 inclusive;

c. Chapter VII of the applied GDPR (remedies, liabilities and penalties)
    i. Article 83 (general conditions for imposing administrative fines);
    ii. Article 84 (penalties);
d. Part 5 of this Act –
    i. Section 112;
    ii. Section 113 (general functions of the Commissioner), subsections (3) and (8);
    iii. Sections 114 – 117;
e. Part 7 of this act, section 173 (representation of data subjects)

(8) Any person **who believes they are** directly **or are indirectly** affected by a certificate under subsection (1)
a. may appeal to the Tribunal against the certificate, and
b. rely upon section 173 of this Act.

(9) If, on an appeal under subsection **(8)**, the Tribunal finds that, ~~applying the principles applied by a court on an application for judicial review,~~ **it was not necessary or proportionate to issue** ~~the Minister did not have reasonable grounds for issuing~~ a certificate, the Tribunal may –
a. Allow the appeal, and
b. Quash the certificate.

(10) ~~Where, in any proceedings under or by virtue of the applied GDPR or this Act, it is claimed by a controller that a certificate under subsection (1) which identifies the personal data to which it applies by means of a general description applies to any personal data, another party to the proceedings may appeal to the Tribunal on the ground that the certificate does not apply to the personal data in question~~.

~~(11) But, subject to any determination under subsection (**8**), the certificate is to be conclusively presumed so to apply.~~

~~(12) On an appeal under subsection (**6**), the Tribunal may determine that the certificate does not so apply.~~

~~(13) A document purporting to be a certificate under subsection (1) is to be –~~
~~a. Received in evidence, and~~
~~b. Deemed to be such a certificate unless the contrary is proved.~~

~~(14) A document which purports states on its face that it is to be a certificate approved by a Judicial Commissioner by or on behalf of a Minister of the Crown as a true copy of a certificate issued by that Minister under subsection (1) and complies with subsection (2) is –~~
~~a. In any legal proceedings, evidence of that certificate;~~
~~b. In any legal proceedings in Scotland, sufficient evidence of that certificate~~

(15) The power conferred by subsection (1) on a Minister of the Crown is exercisable only by –

a. A Minister who is a member of the Cabinet, or
b. The Attorney General or the Advocate General for Scotland.

Clause 26: National security ~~and defence~~: modifications to Articles 9 and 32 of the applied GDPR

(1) Article 9(1) of the applied GDPR (prohibition on process of special categories of personal data) does not prohibit the processing of personal data to which this Chapter applies to the extent that the processing is carried out –

a. For the purpose of safeguarding national security ~~or for defence purposes~~, and
b. With appropriate safeguards for the rights and freedoms of data subjects.

~~(2) Article 32 of the applied GDPR (security of processing) does not apply to a controller or processor to the extent that the controller or processor (as the case may be) is processing personal data to which this Chapter applies for –~~

~~a. The purpose of safeguarding national security, or~~
~~b. Defence purposes~~

~~(3) Where Article 32 of the applied GDPR does not apply, the controller or the processor must implement security measures appropriate to the risks arising from the processing of the personal data.~~

(4) ~~For the purposes of subsection (3),~~ **In addition to Article 32 of the applied GDPR** where the processing of personal data is carried out wholly or partly by automated means, the controller or the processor must, following an evaluation of the risks, implement measures designed to –

a. Prevent unauthorised processing or unauthorised interference with the systems used in connection with the processing,
b. Ensure that it is possible to establish the precise details of any processing that takes place,
c. Ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored, and
d. Ensure that stored personal data cannot be corrupted if a system used in connection with the processing malfunctions.

Annex B

Clause 24: exemptions for national security and defence

A full list of what this clause exempts is set out below:

Chapter II of the applied GDPR (principles)

Article 5: lawfulness, fairness and transparency (except 5(1)(a))[13]
~~**Article 6:** Lawfulness of processing~~ (exception 24(2)(a(iI))
Article 7: Conditions for consent
Article 8: Conditions applicable to child's consent in relation to information society services
~~**Article 9:** Processing of special categories of personal data~~ (exception 24(2)(a)(iiI))
Article 10: Processing of personal data relating to criminal convictions and offences
Article 11: Processing which does not require identification

Chapter III: Rights of the data subjects (24(2)(b))

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 13: Information to be provided where personal data are collected from the data subject.
Article 14: Information to be provided where personal data have not been obtained from the data subject.
Article 15: Right of access by the data subject
Article 16: Right to rectification
Article 17: Right to erasure

---

[13] (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for **specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;** 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 ('purpose limitation');

(c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');

(d) **accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(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; 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 ('storage limitation');

(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 ('integrity and confidentiality').

Article 18: Right to restriction on processing
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing.
Article 20: Right to data portability.
Article 21: Right to object
Article 22: Automated individual decision-making including profiling
Article 23: Restrictions

Chapter IV: Controller and Processor (24(2)(c)
Article 33: Notification of a personal data breach to the supervisory authority (24(2)(c)(i))
Article 34: Communication of a personal data breach to the data subject (24(2)(c)(ii))

Chapter V: Transfers of personal data to third countries or international organisations (24(2)(d)
Article 44: General principle for transfers
Article 45: Transfers on the basis of an adequacy decision
Article 46: Transfers subject to appropriate safeguards
Article 47: Binding corporate rules
Article 48: Transfers or disclosures not authorized by Union law
Article 49: Derogations for specific situations
Article 50: International cooperation for the protection of personal data

Chapter VI: Independent supervisory authorities
Article 57: Tasks (57(1)(a) and (h) (24(2)(e)) – Commissioner's duties to monitor and enforce the applied GDPR and to conduct investigations
Article 58: Powers (24(2)(ii)) – investigative, corrective, authorisation and advisory powers of Commissioner

Chapter VIII: Remedies, liability and penalties (24(2)(f))
Article 77: Right to lodge a complaint with a supervisory authority
Article 78: Right to an effective judicial remedy against a supervisory authority
Article 79: Right to an effective judicial remedy against a controller or processor
Article 80: Representation of data subjects.
Article 81: Suspension of proceedings
Article 82: Right to compensation and liability
~~**Article 83:** General conditions for imposing administrative fines~~ (exception 24(2)(f)(i))
~~**Article 84:** Penalties~~ (exception 24(2)(f)(ii))

Part 5 Data Protection Bill
Section 113 – general functions of the Commissioner
(3) The Commissioner's functions in relation to the processing of personal data to which the GDPR applies include—
(a) a duty to advise Parliament, the government and other institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data, and
(b) a power to issue, on the Commissioner's own initiative or on request, opinions to Parliament, the government or other institutions and bodies as well as to the public on any issue related to the protection of personal data.

(8) The following powers are exercisable only by giving an enforcement notice under section 142— (a) the Commissioner's powers under Article 58(2)(c) to (g) and (j) of the GDPR (certain corrective powers); (b) the Commissioner's powers under Article 58(2)(h) to order a certification body to withdraw, or not to issue, a certification under Articles 42 and 43 of the GDPR.
(9) The Commissioner's powers under Articles 58(2)(i) and 83 of the GDPR (administrative fines) are exercisable only by giving a penalty notice under section 148.

Section 117 – inspection in accordance with international obligations

(1) The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2).
(2) The power is exercisable only if the personal data—
    a. is processed wholly or partly by automated means, or
    b. is processed otherwise than by automated means and forms part of a filing system or is intended to form part of a filing system.
(3) The power under subsection (1) includes power to inspect, operate and test equipment which is used for the processing of personal data.
(4) Before exercising the power under subsection (1), the Commissioner must by written notice inform the controller and any processor that the Commissioner intends to do so.
(5) Subsection (4) does not apply if the Commissioner considers that the case is urgent.
(6) It is an offence—
    a. intentionally to obstruct a person exercising the power under subsection (1), or
    b. to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

Part 6
Sections 137 – 147
137: Enforcement notices
138: Information notices: restrictions
139: Failure to comply with an information notice
140: Assessment notices
141: Assessment notices: restrictions
142: Enforcement notices
143: Enforcement notices: supplementary
144: Enforcement notices: rectification and erasure of personal data
145: Enforcement notices: restrictions
146: Enforcement notices: cancellation and variation
147: Powers of entry and inspection

Schedule 15 – Commissioner's notices and powers of entry and inspection

Part 7
Section 173 – representation of data subjects

Annex C
Further background on automated decision-making

Computational algorithms and machine learning
Computational algorithms are perhaps most appropriately defined as *"a series of well-defined step-by-step operations"* performed by a computer.[14] Such step-by-step operations can be used for processes and decision-making on a very large scale. An algorithm could be designed to turn very specific input variables, such as credit card transaction information, into output variables such as a flag for fraud. If the credit card transactions follow a specific pattern, the system could automatically classify the transaction as fraudulent.

Profiling (and automated decision-making) that is based on *machine learning* go further than specified computational algorithms. Rather than explicitly formalizing a model as a single step-by-step algorithm, machine learning trains a model implicitly. Machine learning algorithms learn from and are trained on large amounts of data. In the case of financial transactions, for instance, the designer of a machine learning system would not specify a rule which defines what kinds of transaction patterns indicate a fraudulent account. Instead, machine learning systems learn often highly non-linear correlations from data which is fed into them for training purposes (training data), which is then formalized as a model that can be queried with input data.

Purposes and practical applications
Automated decision-making may occur in a range of contexts, from targeted advertising and healthcare screenings to policing, for a variety of purposes. Examples of combining profiling and decision-making to score, rate and assess people include:

- A hiring software analyses an applicant's voice in order to identify applicants with *"energy and personality"* and evaluates *"language proficiency, fluency, critical thinking, and active listening".*[15]

- In 2016, IBM launched a tool that would help governments separate "real asylum seekers" from potential terrorists by assigning each refugee a score that would assess their likelihood to be an imposter.[16]

- Hiring software automatically scores and sorts resumes and ranks applicants. The hiring company only considers applicants that score above a certain threshold.[17]

- The NSA reportedly uses web browsing data to predict an internet user's likely nationality, which allows the agency to distinguish between foreign and domestic communications.[18]

[14] Michael Negnevitsky, Artificial Intelligence, A guide to intelligent systems, second edition, 2005
[15] http://www.hireiqinc.com/solutions [Accessed 1st August 2017]
[16] Tucker, P., 2016, Refugee or Terrorist? OBM Thinks Is Software Has the Answer. *Defense One*. http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-has-answer/125484/ [Accessed 1st August 2017]
[17] Rosenblat, A. and Kneese, T., 2014. Networked Employment Discrimination.

- In 2013, the Chicago Police Department conducted a pilot of a predictive policing program designed to reduce gun violence. The program included development of a Strategic Subjects List (SSL) of people estimated to be at highest risk of gun violence. Research found that individuals on the SSL are not more or less likely to become a victim of a homicide or a shooting, but are more likely to be arrested for shooting.[19]
- A social networking site automatically flags some names as fake and suspends the respective accounts. As a result of this automated system, a disproportionate number of minorities' names are deleted.[20]

Automated decisions, informed by profiling, may also be made based on a person's individual environment. Real-time personalisation gears information towards an individual's presumed interests. Such automated decisions can even be based on someone's predicted vulnerability to persuasion or their inferred purchasing power.

(a) Social media platforms tailor their services to their users' presumed tastes and interests, including what kinds of content, including news, users see in their news feeds, and in which order.[21]

(b) Billboards on the Tokyo Expressway—on one of Japan's busy expressways—detect and identify cars to then select and display content based on the types of cars.[22]

(c) Another study examined 16 major e-commerce sites and found search discrimination, i.e. differences in the products shown to users based on their click and purchase history as well as their operating system or browser or whether they were using a mobile device.[23]

As we move towards 'smart' environments and 'persuasive computing' automatically modified choice architectures[24] can nudge the behaviour of data subjects in the real world.[25]

---

[18] Cheney-Lippold, J., 2011. A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture & Society*, *28*(6), pp.164-181.
[19] Saunders, J., Hunt, P. and Hollywood, J.S., 2016. Predictions put into practice: a quasi-experimental evaluation of Chicago's predictive policing pilot. *Journal of Experimental Criminology*, *12*(3), pp.347-371.
[20] Kayyali, D., 2015, Facebook's Name Policy Strikes Again, This Time at Native Americans. *EFF.* https://www.eff.org/deeplinks/2015/02/facebooks-name-policy-strikes-again-time-native-americans
[21] Holm, N., 2016. *Advertising and Consumer Society: A Critical Introduction*. Palgrave Macmillan.
[22]https://builders.intel.com/docs/storagebuilders/deep_learning_enables_intelligent_billboard_for_dynamic_targeted_advertising_on_tokyo_expressway.pdf [Accessed 1st August 2017]
[23] Hannak, A., Soeller, G., Lazer, D., Mislove, A. and Wilson, C., 2014, November. Measuring price discrimination and steering on e-commerce web sites. In *Proceedings of the 2014 conference on internet measurement conference* (pp. 305-318). ACM.
[24] Tene, O. and Polonetsky, J., 2012. Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, *11*, p.xxvii.
[25] Mikians, J., Gyarmati, L., Erramilli, V. and Laoutaris, N., 2012, October. Detecting price and search discrimination on the internet. In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks* (pp. 79-84). acm.