BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

THE DATA PROTECTION BILL – BRIEFING

INTRODUCTION:

The Data Protection Bill was published on the 13th September 2017.

Along with the General Data Protection Regulation (GDPR) the Data Protection Bill (DP Bill) is the biggest shake up of Data Protection law in the UK since 1998.

In the UK our data protection laws currently rely on one document The Data Protection Act 1998. The Act, is a reasonably short document which clearly spells out right from the start what a person's data protection rights are.

The new dual laws of the GDPR and the DP Bill are welcome in that they expand and clarify data protection for the 21st Century, but by introducing two separate pieces of law there is the opportunity for confusion for the public to know what their rights are, when they can be used and how.

This briefing outlines the difference between the GDPR and the DP Bill and outlines the welcome aspects of the DP Bill for the public and areas of concern which Parliament should look to query and address.

For further detail about the GDPR and what your personal data protection rights are as a citizen and consumer under the GDPR, please read our GDPR Factsheets www.bigbrotherwatch.org.uk/factsheets

The Data Protection Bill (DP Bill)

The DP Bill will replace the Data Protection Act (1998)

The DP Bill does 4 critical things:

1. It writes into UK law all the areas the UK Government have chosen to derogate (make changes) from the GDPR
2. It writes into UK law the EU Law Enforcement Directive – thereby outlining what your data protection rights are when your personal data is used by the police
3. It writes into UK law the Council of Europe's Convention for the Protection of Individuals with Regards to the Automatic Processing of Personal Data
4. It makes clear that you have **NO** data protection rights when it comes to:
    a. National security
    b. When data is needed for the "public interest" such as media reporting, freedom of information or for research purposes.
    c. If you data is to be used for the purpose of freedom of expression by journalists, artists, writers and academics.
    d. If your data is to be used for statistical, scientific or historical research

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

The General Data Protection Regulation (GDPR)

The GDPR provides a complete update of data protection law for the digital age. It outlines 8 rights citizens have over their personal data.

The 8 rights are:

1. Right to be informed
2. Right of access
3. Right to object
4. Right to rectification
5. Right to erasure
6. Right to portability
7. Right to restrict processing
8. Right to challenge automated decision making and profiling

The GDPR is an EU regulation which must be enforced by all EU Member States, including the UK up to and hopefully beyond Brexit.

The GDPR will come into force in the UK on the 25th May 2018.

Because the UK has voted to leave the European Union and the GDPR is an EU regulation, once the UK formally "Brexit's", the GDPR will become subject to the EU(Withdrawal) Bill, should that Bill become an Act.

This means that post Brexit, the data protection rights outlined in the GDPR, which are not outlined in the Data Protection Bill, will need to be written into UK law. If that is not undertaken UK citizen's data protection rights will be weakened and the UK as a whole will be seen as inadequate as a country which data can be shared to and from.

Knowing your rights under the Data Protection Bill and the GDPR

If you want to know what your data rights are when it comes to sharing data with a company, business, organisation or public service you should read the GDPR to get a full sense of your 8 data protection rights and read the Data Protection Bill as a supplementary document. For an overview of the GDPR a citizens rights please read our GDPR Factsheets at https://bigbrotherwatch.org.uk/factsheets/gdpr-factsheets/

If you want to know your rights in relation to data being held and used by the police or the intelligence agencies you will need to read the Data Protection Bill.

If you want to know your rights when your data is being held and used for the purpose of research and statistics, or when personal data is being used as a matter of public interest, you will need to read the Data Protection Bill.

We would recommend that you familiarise yourself with both documents to be 100% clear on your data protection rights as a whole.

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

PART 1 – PRELIMINARY

Part 1 Introduces the Bill.

Part 1 makes clear the complexity of the full data protection laws which are relevant to UK citizens.

The overview[1] says that *"most processing of personal data is subject to the GDPR"* – making clear from the outset that anyone wanting to know the very basic details of what their data protection rights are will need to consult a different document.

And later on,[2] the Bill lists all the *"data protection legislation",* which includes: *"The GDPR, the applied GDPR, this Act, regulations made under this Act".* Hardly straightforward.

PART 2 - GENERAL PROCESSING

Part 2 of the Bill addresses how most data will be processed. It sets out how the UK intends to implement the GDPR and outlines where the UK Government has chosen to make exemptions to the GDPR. It offers details of definitions and terms such as the meaning of "controller" and the meaning of "public authority" and "public body" and details some of the rights an individual has to their personal data.

Section 3 requires citizens, business and organisations who want to know their rights and obligations under the Bill to cross reference and read the Bill alongside the GDPR, potentially creating confusion and the possibility of undermining data protection in the process.[3]

It is worth noting **Section 13** which outlines the safeguards being put in place to protect people from automated decision making. This is important as automated decision making, such as artificial intelligence and algorithms, will become a critical feature of how our data is analysed going forward.

The exemptions detailed in **Section 14** make clear that many of the rights the GDPR provides to people over their personal data such as rights to access personal data, to rectification of personal data, the right to erasure, restriction of processing, and to object to automated decision-making do not apply when it comes to issues of national security, public interest, areas of research and freedom of speech in relation to journalism, art, literary purposes or academic purposes.

Section 14 sets the tone for what is to follow in Parts 3 and 4 of the Bill.

Section 18 is a clause we hope Parliament look closely at as the Bill progresses. The way the clause is drafted is confusing and could lead to errors being made.

Section 18 details the way data is processed for archiving, research and statistical purposes.

Section 18(2) states that:

[1] Section 1(2)
[2] Section 2(9)(a) to (e)
[3] Section 3(2)(b)

"Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if—

> *(a) it is carried out for the purposes of measures or decisions with respect to a particular data subject, or*
>
> *(b) it is likely to cause substantial damage or substantial distress to an individual."*

The clause is worded in such a way as to give effect to a privision of the GDPR, but can be read as follows: *"Such processing does not satisfy the requirement… for the processing to be subject to appropriate safeguards… if – … (b) it is likely to cause substantial damages or substantial distress to an individual*".

This suggests that if processing is for archiving purposes in the public interest, scientific or historical purposes, or statistical purposes, it does not need to be subject to appropriate safeguards if it is likely to cause substantial damage or distress to an individual.

We doubt this is the actual intended meaning. Because the same issues are referenced in Section 39 of the Bill in relation to law enforcement in a much clearer way, we recommend that consideration be given to amending Section 18 to read in the same way as Section 39 in order to prevent misinterpretation or confusion.

Section 25 is important as it allows a Minister to sign and issue a certificate which makes any of the rights or punishments of the GDPR or the Data Protection Bill meaningless if there is a need to access personal data for the purpose of safeguarding national security.

A certificate can be issued which can have a long term effect and it can be issued on what is described as a *"general description"* meaning that any or all personal data can be looked at.

Section 25 does offer individuals affected by a national security certificate the right to appeal to a Tribunal,[4] but the irony of this protection is that it may be impossible for an individual to ever find out their data was subject to a national security certificate.

The lack of notification for citizens when it comes to knowing what happens to their personal data, particularly in relation to how their data can be accessed by the intelligence agencies; namely MI5, MI6 and GCHQ and in some cases HMRC is an ongoing problem and one we have raised during the passing of the Investigatory Powers Act.

The opportunity for rights to be halted and offences to be of no consequence when it comes to personal data, are littered throughout the Data Protection Bill.

Section 26 is worth noting. It makes clear that the intelligence agencies have to ensure that all data is protected, that the processing of any data is precisely detailed, that data must not be processed or interfered with without authorisation. This is a welcome protection.

[4] Section 25(3)

PART 3 – LAW ENFORCEMENT PROCESSING

Part 3 addresses how data will be processed by law enforcement in the UK.

We welcome a number of provisions which protect citizens' data and which enhance how citizens are informed or notified about how their data is processed when it comes to law enforcement processing of data.

Section 55 (Data protection by design and default) is a welcome move designed to ensure that the police take the protection of data retained in their systems seriously.

This is particularly important when you consider that as the police adopt greater technological advancements for everyday frontline policing, the volume of personal and sensitive data, including video, audio and biometrics of citizens is only going to increase. Ensuring such sensitive data are protected by systems designed to be secure by default is a positive step forward. We hope that investment in police IT systems permits this clause to be enacted without delay.

Section 59 (Records of processing activities) and **Section 60** (Logging): These two clauses require the police to keep records of how they process personal data and activities, and that automated processing system operations are logged.

This should ensure that data gathered from technological advancements, such as surveillance cameras, biometrics, audio etc, are recorded and logged. This is necessary to ensure police transparency, not only in relation to how they acquire and handle such personal data, but also to ensure that an audit can be undertaken to show clearly how, when and why personal data of this nature is shared, used and destroyed.

We have raised concern about the current lack of logging and auditing of data obtained through new technologies in a recent report about police use of Body Worn Cameras.

Section 62 (Data protection impact assessment), **Section 63** (Prior consultation with the Commissioner), and **Section 67** (Designation of a data protection officer): All three of these clauses place emphasis on the police to ensure that, before undertaking any new approach to policing and law enforcement which might involve data, they step back and consider the impact on a person's privacy, security and data protection before going ahead with the proposal. By having to engage with the Information Commissioner and undertake a privacy impact assessment the issue of data protection as a part of good policing should be ever present.

The need for the police to have specific data protection officers to oversee any handling, retention, sharing or interrogation of data is a positive step.

Section 66 (Communication of a personal data breach to the data subject): This section rightly requires the police to tell people if their personal data has been breached.

Whilst this is a great move to ensure transparency and also notification to the public about what happens to their data, we are concerned that there are exemptions to the rule.

Section 66(3) gives the police permission not to notify people about a data breach if they consider it to *"involve a disproportionate effort"*.[5]

This is not defined any further, so we have no idea what a disproportionate effort means.

By offering such a broad definition for when a data breach does not have to be reported we are concerned that it could be used as an excuse for the police not to notify people about serious data breaches.

Section 66(7) provides an even wider exemption for when the police are exempt from notifying a person about a breach of their data held by the police. The exemptions are permitted if notifying the citizen would impact the police's ability to:

- "*protect public security*";
- "*protect national security*"; and
- "*protect the rights and freedoms of others*".[6]

We acknowledge that the exemptions are specific and relate to the impact notification could have on a specific case or an issue of national/public security. But we believe that whenever possible, after a court case has ended or any specific threat has passed, innocent citizens should be notified if a breach of their data has occurred.

PART 4 – INTELLIGENCE SERVICES PROCESSING

Part 4 outlines the protections available to citizens when it comes to the processing of data by the Intelligence Services – GCHQ, MI5 and MI6 and in part where tax affairs are considered, the processing of data by HMRC.

Chapters 1 – 5 outline a broad range of data protection rights for citizens. Specifically:

- **Section 92:** Right of access
- **Section 94:** Right not to be subject to automated decision-making
- **Section 95:** Right to intervene in automated decision-making
- **Section 96:** Right to information about decision-making
- **Section 97:** Right to object to processing
- **Section 98:** Rights to rectification and erasure

All these clauses are welcome rights in Part 4 of the Bill, but they are unfortunately all rendered obsolete by the comprehensive restrictions and exemptions set out in **Section 108** in Chapter 6 of Part 4 of the Bill.

[5] Section 66(3)(c)
[6] Section 66(7)

Section 108 (National security exemption) provides a general exemption from all of the data protection principles and the data subjects' rights in Part 4 of the Bill if it is *"required for the purpose of safeguarding national security",* thereby rendering all of the principles and rights in Part 4 of the Bill meaningless.

Arguably, data protection rights in relation to the intelligence agencies will apply to employees of the intelligence services, in order to ensure that their personal data in relation to their employment is being protected. It certainly doesn't apply to citizens as a whole.

Despite the broad undermining of protections, it is worth taking note of **Section 88** (The fifth data protection principle).

Section 88 permits the intelligence agencies to effectively hold data for an undefined period of time. It states that "*personal data must be kept for no longer than is necessary for the purpose for which it is processed"* but it does not include any time limits for review on the retention of people's personal data, meaning that innocent people's personal data could be held indefinitely. This is at odds with the rules for law enforcement who are required to review how long data is held for. We would prefer to see similar requirements for the intelligence agencies, to ensure that independent oversight of procedures in relation to data retention have more nuanced time frames.

PART 5 – INFORMATION COMMISSIONER

Part 5 of the Bill outlines the *"general functions"* of the Information Commissioner.

The Information Commissioner is the independent body overseeing data protection in the UK.

Section 118 (Further international role) is an important clause to take note of in this Part. Whilst the UK is part of Europe the Information Commissioner has a seat at the table of data protection leads from all other EU Member States. Once we Brexit that seat will be removed.

This is a critical point which should be acknowledged, particularly in relation to the UK's data protection laws post Brexit and the UK achieving the high standard of adequacy.

ADEQUACY

The issue of adequacy after the UK leaves the European Union is absolutely critical for the UK in a post Brexit time.

Currently, countries in the European Economic Area (EEA) (an area in which goods and services pass freely between countries, which includes all EU countries and a few others) can only transfer data between themselves because they all have to adhere to the same high standards of protection around personal data and its transfer. In other words countries have, by complying with the same data protection laws, reached an agreed level of adequacy.

However, if one of those countries wants to transfer personal data *outside* the EU or EEA, it can only do so if a similar *"adequate"* level of protection of that personal data is guaranteed by the external

country.[7] Whether or not a country's data protection regime is considered adequate is down to its domestic laws or the international commitments it has entered into.[8] Adequacy decisions are made by the EU Commission.

Because the UK will be leaving the EU in May 2019, the UK will have to prove its data protection laws and practices reach the required level of adequacy, in order for us to share and receive data with EU and EEA countries.

The Information Commissioner has made clear that the *"best way forward"* after Brexit is for the UK *"to achieve an adequacy finding"* with the European Union.[9] However, adequacy is not guaranteed.

The introduction of this new Data Protection Bill will be key to the UK reaching data protection adequacy. However there are some serious points which may impact us reaching adequacy:

1. If the GDPR is amended or written out of UK law under the European Union (Withdrawal) Bill.
2. If elements of this Bill where the UK has set its own agenda, away from EU standards, are considered not to protect peoples data sufficiently. For example, where citizens are not able to exercise their right to appeal against restrictions being placed on their rights under this Data Protection Bill.[10]
3. Provisions in the Investigatory Powers Act which allow the police to access personal data such as communications data or internet data without the requirement for independent judicial approval, and without any requirement for the issue being investigated to be of a certain level of seriousness. In such a context, the general, indiscriminate and bulk data retention powers available under the Act are also highly invasive and problematic.

If the GDPR is significantly altered during the repeal process under the European Union (Withdrawal) Bill, and citizens' personal data rights are **not** enshrined in the Data Protection Bill, this could leave us a very long way away from the necessary levels of data protection required by the EU to be viewed as adequate.

We are concerned that elements of this Bill, specifically the restrictions and modifications made in it, may not allow a sufficient level of data protection for UK citizens' personal data.

The Information Commissioner has specified that in order for the UK to achieve *"the gold standard of data protection regulation and enforcement",* then *"the right way forward… is to fully adopt the GDPR".* The UK Government must ensure that it protects UK citizens' personal data protection rights and the obligations due to them by data controllers or processors.

---

[7] http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm
[8] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[9] Elizabeth Denham, House of Lords EU Home Affairs Sub-Committee, Wednesday 8 March 2017 http://www.parliamentlive.tv/Event/Index/125e1463-62ed-41bb-ab64-811d0f94bfee
[10] For example: Sections 23(3). Section 66(3)(c) or 66(7), Section 77(5), and Section 108

Government can do this by:

1. Ensuring that the GDPR is enshrined in UK law and, specifically, written into this Bill, in order to protect against its being watered down or done away with by post-Brexit repeals during the 'transition' phase.
2. Ensuring that all elements of this Bill are compatible with EU standards of data protection, and that it does not allow sections to unjustifiably remove individuals' rights.
3. Ensuring the UK's surveillance and bulk data retention regime under the Investigatory Powers Act 2016 is compatible with EU standards.

With regard to point 3, the ruling of the Court of Justice of the European Union (CJEU) earlier this year in *Watson*[11] with regards to the UK's surveillance and bulk data retention regime, is extremely important.

The decision by the CJEU in *Watson* clearly stated that the UKs surveillance and data retention laws, then codified in the Data Retention and Investigatory Powers Act (DRIPA) 2014, exceeded the limit of what is strictly necessary and could not be considered justified, in a democratic society.[12] This model of retaining communications data is broadly mirrored in the new Investigatory Powers Act 2016, the replacement for DRIPA. If the UK does not ensure that its new data protection regime as set out in this Bill is in line with the EU's adequacy requirements, to the very minimum standards espoused by the CJEU, the EU may not consider that the UK reaches adequacy.

UK data sharing with other (non-EU) countries

There is a further issue with the UK sharing citizens' personal data with countries who don't reach adequacy. If the UK shares UK citizens' personal data with countries which don't reach adequacy or which do not have a sufficient level of protection in place for such data, this could potentially infringe on citizens' human rights or their safety and security. For example, this could happen if such personal information was compromised through data loss, breach, or hacking.

Transferring personal data through insecure frameworks undermines rights and safety; whilst the UK should ensure its own framework is secure and adequate, it must also ensure that those countries with which it shares personal data also have adequate frameworks.

PART 6 – ENFORCEMENT

Part 6 details the penalties organisations will suffer if they don't adhere to the data protection rights and obligations

Section 150 (Maximum amount of penalty) is a very welcome brand new addition to data protection. Currently the maximum fine that can be imposed on an organisation for breaching data protection laws is £100,000. This is for some organisations a phenomenal amount of money, but for many others,

[11] Joined Cases C 203/15 and C 698/15 *Tele2 Sverige AB v Post- och telestyrelsen,* and *Secretary of State for the Home Department v Tom Watson MP, Peter Brice and Geoffrey Lewis*
http://curia.europa.eu/juris/document/document.jsf?docid=186492&doclang=EN
[12] *Ibid*

particularly those whose business model relies solely on data, it is fairly small. It therefore provides no deterrent or encouragement for organisations to adhere to and maintain strong data protection. Section 150 has substantially bolstered the level of fine which can be issued by the Information Commissioner to an organisation who has been involved in a data breach. Now an organisation can be fined either 20 million Euros or 4% of the organisation's annual turnover, whichever is higher. This makes very clear that those who do not handle our data properly and securely will face significant financial penalties.

There are a few clauses in Part 6 which we believe warrant further clarification as the Bill progresses through Parliament, most notably:

Section 162 (Re-identification of de-identified personal data) specifically Section 162(4)(a)(iii) appears to allow a person who has re-identified de-identified data to claim in their defence that *"the person – would have had such consent if the data subject had known about the re-identification and the circumstances of it."*

It seems odd that assumed consent is permitted as a defence, particularly when the issue of consent is pretty strong throughout the GDPR.

It would be helpful to determine what is exactly meant by this clause.

Section 163 (Alteration etc of personal data to prevent disclosure), specifically Section 163(5)(a) which states that: *"It is a defence for a person charged with an offence under subsection (3)to prove that –*

(a) the alteration, defacing, blocking, erasure, destruction or concealment of the information would have occurred in the absence of a request made in exercise of a data subject access right"

This clause appears to allow for alteration of personal data to be carried out on receipt of a disclosure request if *"the controller or a person who is employed by the controller"* can prove merely on the balance of probabilities that they were going to do it anyway.

As with Section 162 it would be helpful to determine exactly what is meant by this clause.

PART 7 – SUPPLEMENTARY AND FINAL PROVISIONS

Part 7 of the Bill outlines a number of clauses which don't clearly fit into the earlier defined parts and chapters.

Section 173 (Representation of data subjects) is a clause which enables an individual who believes they have been a subject of a data breach to approach an independent organisation who specifically works in the area of data protection, and ask for their assistance in representing them with raising a complaint to the Information Commissioner.

Section 177 (Liability of Directors) places responsibility on individuals within organisations for data breaches. If you consider recent large scale data breaches at huge organisations such as Equifax and Talk Talk, Section 77 ensures that individuals at the top of the company can be held to account for poor data protection across the organisation as a whole.

Section 178 (Recordable offences) is a very positive step forward. Whilst it does not implement our long-standing calls for custodial sentences to be issued to those who are found guilty of serious data breaches or lapses of data protection it is still a welcome step.

Section 178 makes data offences a recordable offence, meaning that individuals who have been found to be responsible within an organisation for a data breach or misuse of data will have the offence recorded as a police record.