Title: Data Protection Bill: summary assessment **IA No: DCMS2017** **RPC Reference No.** **Lead department or agency:** Department for Digital, Culture, Media and Sport **Other departments or agencies:** Home Office	**Impact Assessment (IA)** **Date:** 07/09/2017 **Stage:** Final **Source of intervention:** Domestic **Type of measure:** Primary legislation **Contact for enquiries:** dataprotectionbill@culture.gov.uk

Summary: Intervention and Options

RPC Opinion: Not Applicable

Cost of Preferred (or more likely) Option				
Total Net Present Value:	**Business Net Present Value**	**Net cost to business per year** (EANCB in 2017 prices)	**One-In, Three-Out?**	**Business Impact Target Status**
-	-	-	In scope	Non-qualifying provision

What is the problem under consideration? Why is government intervention necessary?

The Data Protection Act 1998, which provides our legal framework for data protection in the UK, is now 20 years old and needs updating to reflect the changes in the way data is generated and used in the digital world. With the increasing volumes of personal data held by businesses and government there is an increasing need to protect and to create strong data protection laws and appropriate safeguards. The Bill will do this and also ensure that, following the UK's exit from the EU, our criminal justice agencies can continue to share data with other EU Member States to tackle crime and threats to our security.

What are the policy objectives and the intended effects?

To provide a comprehensive and modern framework for data protection in the UK, with stronger sanctions for malpractice. To set new standards for protecting general data, in accordance with the GDPR, give people more control over use of their data, and provide new rights to move or delete personal data whilst preserving existing tailored exemptions from the Data Protection Act. It is also intended to provide specific frameworks tailored to the needs of our law enforcement agencies and intelligence services, to protect the rights of victims, witnesses and suspects while ensuring we can tackle the changing nature of global threats.

What policy options have been considered, including any alternatives to regulation? Please justify preferred option (further details in Evidence Base)

Option 1 – Do nothing: this option does not meet the Government's objective. The EU General Data Protection Regulation (GDPR), as a directly applicable regulation, would apply in the UK but so too would the 1998 Act, causing legal uncertainty and confusion for both individuals and organisations in applying the law. Without exercising some of the available derogations in the GDPR and LED, we would be failing to minimize burdens on organisations.

Option 2 – Create a new law: Replace the Data Protection Act with a new comprehensive regime for protecting personal data, including implementation of the GDPR, transposing the LED and exercising the derogations in the best interest of the UK.

Will the policy be reviewed? It will be reviewed. If applicable, set review date:

Does implementation go beyond minimum EU requirements?		No		
Are any of these organisations in scope?	**Micro** Yes	**Small** Yes	**Medium** Yes	**Large** Yes
What is the CO_2 equivalent change in greenhouse gas emissions? (Million tonnes CO_2 equivalent)		**Traded:** N/A	**Non-traded:** N/A	

I have read the Impact Assessment and I am satisfied that (a) it represents a fair and reasonable view of the expected costs, benefits and impact of the policy, and (b) that the benefits justify the costs.

Signed by the responsible Minister: Date: 12 September 2017

Background

A. Strategic Overview

The UK is at the forefront of data innovation and the UK data economy continues to grow in both size and significance. Analysis predicts that data will benefit the UK economy by up to £241 billion between 2015 and 2020.[1] In this context, in order to guarantee the UK's continued growth and prosperity, and maximize future trading opportunities, it is crucial that we are able to guarantee effective, unrestricted data flows.

The Data Protection Act 1998 (DPA 1998), which provide the legal framework for data protection in the UK, is now 20 years old and needs updating to reflect the changes in the way data is generated and used in the digital world. With the increasing volumes of personal data held by businesses and government there is an increasing need to protect it. Data loss can often have distressing repercussions on individuals whilst risking significant reputational damage for the responsible party and the victims lose trust. In more serious cases significant financial loss can arise on both sides and there are risks of other serious harms.

Currently, an individual's personal data is protected in the UK by the DPA 1998, internationally recognised as a gold standard. Since then there have been numerous technological developments, notably the rapid expansion of the internet, the emergence of social media and the growing importance of smart phones.

In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU, which were in large part, intended to give EU citizens back control of their personal data. Negotiation influenced the final official texts of the General Data Protection Regulation (GDPR) and the Data Protection Directive (commonly known as the Law Enforcement Directive (LED)) which were published on 4 May 2016 in the EU Official Journal. The final texts include a number of flexibilities that the UK negotiated. The UK Government is keen to bring the GDPR and LED into force with the safeguards and exemptions embedded in the DPA. This will ensure that the burden on business is kept minimal while a high standard of protection of individuals' data is guaranteed.

The LED seeks to provide consistent high level data protection in order to facilitate data sharing between the competent authorities of different EU Member States. It is with this in mind that the LED aims to create an equal level of protection to the rights and freedoms of natural persons across the EU and to remove barriers to data sharing that occur where different countries apply different standards of protection. In transposing the LED provisions into domestic legislation it is intended that this will promote judicial cooperation in criminal matters and police cooperation between the UK and EU Member States.

National Security is outside the scope of EU law, the Bill therefore provides for a specific data protection regime for the processing of personal data by the intelligence services based on the standards on the modernised Council of Europe data protection Convention (Convention 108).

[1] CEBR & SAS (2016), The Value of Big Data and the Internet of Things to the UK Economy, https://www.sas.com/content/dam/SAS/en_gb/doc/analystreport/cebr-value-of-big-data.pdf

B. Groups Affected

Data protection laws primarily impact on:

- Data controllers and processors[2] in the public, private and third sector (e.g. charities, voluntary organisations). “Data controller” means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. A data controller must be a “person” recognised in law, that is to say individuals; organisations; and other corporate and unincorporated bodies of persons. Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. The LED provisions apply to competent authorities. A competent authority is a public body competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (here in referred to as Law Enforcement Purposes (LEPs)), and any private body entrusted by UK law to perform one of those purposes.

In relation to personal data,

- “Data processor”, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. “Processing”, in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.
- Data subjects whose personal data is processed by UK organisations and UK residents whose personal data is being processed by non-UK organisations. A data subject is an individual who is the subject of personal data.
- Information Commissioner’s Office (ICO), the data protection regulator, with primary responsibility to regulate the GDPR proposals, including investigation of potential breaches and enforcement of information law.
- The justice system as a means through which data related disputes are resolved, particularly in relation to enforcement of new rights and contract breaches within and across Member States; wider society.

C. Options

Option 1 is to make no changes (do nothing)

Option 2 is to use primary legislation to replace existing data protection legislation that will make provision for the GDPR derogations and transpose the LED. This will ensure that the UK continues to have complete and comprehensive data protection laws.

D. Costs and Benefits

This section provides a narrative that summarises the costs and benefits of the Bill where particular impacts have been identified and an impact assessment prepared. Two detailed assessments have been prepared on policy related to this Bill covering general data processing and law enforcement data processing. The NPVs of each measure have not been summed as this does not give an appropriate NPV for the Bill. In some of the impact assessment it has not been possible to quantify the benefits; therefore an overall NPV may be misleading. The individual impact assessments should be consulted for

[2] A data processor' is defined in the GDPR as a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller Usually the data controller who controls the data also processes the data.

further detail on the costs and benefits. All of the individual impact assessments will be published and will be accessible from the Data Protection Bill webpage on GOV.UK[3].

Non-Monetised Benefits

The Bill will bring significant benefits to those impacted by it. However, the majority of the benefits are ones that cannot be monetised. The Department for Digital, Culture, Media and Sport (DCMS) commissioned a report by London Economics to look at the benefits arising from the GDPR[4]. This highlighted that through a consumer choice experiment that individuals would be willing to forego savings of roughly 5 per cent to 10 per cent on weekly spending on shopping, monthly spending on electricity or monthly spending on health insurance in order to have the rights enshrined in the GDPR. This indicates clearly that individuals place a significant value on the benefits attached with having greater consumer trust in the digital economy and the extra rights gained from the GDPR which include:

- Easier rights of access to one's personal data.
- The right to rectification and erasure of one's personal data.
- The right to data portability.

In terms of the permissible derogations allowed in the GDPR which will be exercised through the Data Protection Bill 2017 there are a number of non-monetised benefits gained through the deregulatory effect of utilising the exemptions, these are:

- Organisations that process special categories of data on public interest grounds will be able to continue to do so. This helps to avoid greater risks of fraud to the insurance sector and will further help to avoid the creation of potential barriers to care services and patient safety.
- Industries will be able to continue to process criminal data and continue completing Data Barring Service checks and processing of suspicious activity reports. This will save them the cost of having to hire other businesses to complete these actions. Insurance companies will be able to continue to underwrite claims lending decisions and maintain their risk levels.
- New criminal sanctions will be introduced to ensure the worst breaches of data security are prosecuted. These new sanctions criminalise the illegal decryption of anonymised files.
- The Bill will bring legal certainty and maintain the balance between data protection rights and the rights with regard to the freedom of expression.
- The Bill will also include safeguards and derogations relating to the processing of personal data for archiving purposes in the public interests, scientific or historical research or statistical purposes allowing such works to continue unimpeded.Allowing teenagers from the age of 13 to give consent to access Information Society Services (ISS) will align the UK policy with the US and will increase conversations between parents and children about data protection.

In terms of the LED provisions to be transposed into the Act the crucial non-monetised benefits are the continued ability to facilitate the smooth sharing of personal data for law enforcement purposes with the EU (and its Member States) and others, and the enhanced rights and protections for members of the public whose personal data is held by a competent authority for a law enforcement purpose.

Monetised Benefits

Both the detailed impact assessments that this document summarises contain some discussion around monetised benefits however they are a small proportion of the overall benefits. In terms of the LED the

[3] https://www.gov.uk/government/collections/data-protection-bill-2017

[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635701/PersonalDataRights_LE_-_for_Data_Protection_Bill__1_.pdf

key monetised benefits are around the savings made to consumers from not having to pay a fee for Subject Access requests (SARs) and the reduced risk of serious breaches as a result of stronger data protection measures. In terms of the GDPR the costs saved to private organisations that process data for specific public interests not having to comply with SARs has been calculated.

Costs

The cost to organisations is more readily estimated than the benefits. The Ministry of Justice (MoJ) issued a call for evidence in February 2012[5] and produced an impact assessment[6] as part of the resultant Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework[7] in November of the same year. MoJ looked at the social costs and benefits of the data protection proposals as they were estimated to be at that time based on the proposed legislative framework. Following the published proposals by the European Commission in January 2012 there have been four years of negotiations which led to the adoption of the GDPR and LED by the Council of Europe. DCMS have created an impact assessment (IA) which looks at the permissible derogations from the GDPR that ensures the Bill creates a data protection regime that balances the rights of individuals and the needs of organisations. The DCMS IA does not monetise any potential costs associated with these derogations nor does it monetise the potential costs to data subjects due to the limitation of rights due to processing based on public interest grounds.

The Home Office have produced an impact assessment looking at the costs associated with transposing the LED into domestic legislation. Through a survey of stakeholders information was gathered that allowed certain costs to be estimated based upon a series of economic assumptions. In terms of the LED the key monetised costs are:

- The costs of upgrading systems to comply with the new requirements.
- The costs of ensuring systems have all the required features.
- The lost revenue from fees for SARs.
- The costs of processing increased numbers of SARs.
- The costs of producing Data Protection Impact Assessments (DPIAs).
- The costs to the Information Commissioner's Office (the regulator).

There are some other potential costs associated with the LED which would hold for the GDPR as well. These costs are non-monetised due to a lack of data and cover any additional costs from handling paper files, additional requirements for data sharing, the change in response time for SARs, an expected increase in complaints about SARs, upgrading to prevent unauthorised processing of data, and the cost of increased complaints to the ICO.

E. Risks, Enforcement, Recommendations, Implementation, Evaluation

Risks associated with the preferred options are addressed in both IAs as is enforcement of the preferred option (to create primary legislation that will apply the required derogations to the GDPR and transpose the LED in a way that meets the operational needs of the criminal justice agencies whilst balancing the rights of data subjects). There will be subsequent evaluations of the impact of the Bill as laid out in the separate detailed impact assessments.

[5] https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/summary-responses-proposed-data-protection-legislation.pdf

[6] https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf

[7] https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/ summary-responses-proposed-data-protection-legislation.pdf