Title: Data Protection Bill: implementing the European Union Law Enforcement Directive **IA No: HO0295** **RPC Reference No.** **Lead department or agency:** The Home Office **Other departments or agencies:** The Department of Digital, Culture, Media and Sport, and The Ministry of Justice	**Impact Assessment (IA)** **Date:** 26/10/2017 **Stage:** Final **Source of intervention:** European **Type of measure:** Primary legislation **Contact for enquiries:** Gregor Jack, CPFG gregor.jack@homeoffice.gsi.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** (EANDCB in 2017 prices)	**One-In, Three-Out?**	**Business Impact Target Status**
-£96.0m	N/A	N/A	In scope	Non Qualifying

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

The European Union Data Protection Directive 2016/680 (LED) repeals the Council Framework Decision 2008/977/JHA and needs to be transposed into domestic law to take effect from May 2018 replacing existing data protection legislation in relation to personal data processing for law enforcement purposes.

Only the Government can, through legislative action, ensure that there will be a single data protection regime for law enforcement purposes as defined and covered by the LED for both domestic processing and international transfers. Failure to act could lead to a breach of European legislation and may incur a penalty.

What are the policy objectives and the intended effects?

There has been a significant increase in the collection and sharing of personal data for law enforcement purposes. The policy objective is to ensure secure sharing of personal data between competent authorities within the UK, with the EU and with other countries whilst maintaining a strengthened degree of protection for personal data. The LED seeks to build a strong and more coherent framework for the protection of personal data. The LED, whilst a robust regime, allows for derogations from the rights of data subjects to take account of the operational requirements of law enforcement agencies. In transposing the LED into domestic legislation it is intended to utilise the derogations to meet the UK requirements.

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 and may breach EU law.

Option 2 – Implement the LED using domestic legislation.
Primary legislation will be enacted to transpose the LED into UK law and to repeal existing data protection legislation. The LED will bring clarity to the legal framework, maintain the Information Commissioner's Office (ICO) as the supervisory body and provide a robust regime for the regulation and safeguarding of the use of personal data in a law enforcement context. It can be introduced in a way to ensure the best interests of the UK and the EU are met through the mutal recognition of each others data protection frameworks from the point of exit, and also ensuring future data sharing arrangements have adequate protection and are compatible with our data sharing partners.

Will the policy be reviewed? It will be reviewed. If applicable, set review 04/2022

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: Williams of Trafford Date: 26 October 2017

Summary: Analysis & Evidence

Policy Option 2

Description: Data Protection Bill: Law Enforcement Directive Economic Impact Assessment.

FULL ECONOMIC ASSESSMENT

Price Base Year 2017	PV Base Year 2017	Time Period Years 10	Net Benefit (Present Value (PV)) (£m)		
			Low: -£46m	**High:** -£178m	**Best Estimate:** -£96m

COSTS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Cost (Present Value)
Low		10	£6.7m	**£58m**
High			£22.3m	**£192m**
Best Estimate			£12.7m	**£109m**

Description and scale of key monetised costs by 'main affected groups'

All costs fall to relevant law enforcement agencies, which are mostly public bodies, but could impact on certain private businesses. The main monetised costs are: the costs of upgrading systems to comply with new requirements; the cost of ensuring systems have all required features; lost revenue from fees for subject access requests (SARs); cost of processing increased numbers of SARs; cost of producing data protection impact assessments (DPIA); costs to the Information Commissioner's Office (ICO, the regulator).

Other key non-monetised costs by 'main affected groups'

Public sector bodies and private businesses processing under the LED could incur additional costs from handling paper files, additional requirements for data sharing, change in response time for SARs, expected increase in complaints about SARs, upgrading to prevent unauthorised processing of data, and the cost of increased numbers of complaints to the ICO.

BENEFITS (£m)	Total Transition (Constant Price)	Years	Average Annual (excl. Transition) (Constant Price)	Total Benefit (Present Value)
Low			£1.4m	**£11.6m**
High			£1.7m	**£14.4m**
Best Estimate			£1.5m	**£13.0m**

Description and scale of key monetised benefits by 'main affected groups'

Fees for SARs are abolished (as under the LED they can no longer be charged for a SAR; save in exceptional circumstances), which takes revenue away from the competent authorities but saves the cost of processing the payments.

Reduced risk of serious breaches as a result of stronger data protection measures; this benefit falls to the general public.

Other key non-monetised benefits by 'main affected groups'

The crucial non-monetised benefits of the LED are the continued ability to facilitate 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 any competent authority for a criminal law enforcement purpose.

Key assumptions/sensitivities/risks **Discount rate (%)** 3.5

There is a significant risk that valuations overestimate the impact on public sector authorities because the sample for which we received results is not representative of the wider population. The Home Office received no responses from local authorities,who are likely less to be affected than the agencies for whom we do have data. Total cost is especially sensitive to the volumes of data controllers, particularly in the private sector. Values are based on strong assumptions subject to sensitivity analyses.

BUSINESS ASSESSMENT (Option 2)

Direct impact on business (Equivalent Annual) £m:			Score for Business Impact Target (qualifying provisions only) £m:
Costs: N/A	**Benefits: N/A**	**Net: N/A**	

Evidence Base (for summary sheets)

A. Strategic Overview

A.1 Background

The Ministry of Justice (MoJ), which was then the department responsible for data protection policy, issued a call for evidence in February 2012[1] and produced an Impact Assessment (IA)[2] as part of the resultant Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework[3] in November of the same year. The MoJ IA 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 General Data Protection Regulations (GDPR) and the Law Enforcement Directive (LED) by the Council of Ministers and the European Parliament in April 2016 (the EU data protection package). The Department for Digital, Culture, Media and Sport (DCMS) are leading on the Data Protection Bill which will include legislative provisions to transpose the LED into domestic law. Annex A contains details of the main differences between the LED, the GDPR and the Data Protection Act 1998 (DPA). Annex B discusses the links between the LED and the Investigatory Powers Act 2016.

A.2 Groups Affected

The LED applies to **competent authorities**, in both the private and public sectors, who process personal data for the purposes of 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 (herein referred to as 'law enforcement purposes' (LEPs)). A competent authority is any public authority competent for LEPs, or a private body entrusted by "Member State law" (in this situation that is taken as meaning UK domestic law) to exercise public authority and public powers for LEPs in the capacity of a data controller. This limited definition of a competent authority mostly focuses on public authorities but does include private companies, such as train operating companies when acting in their capacity as a public prosecutor, and the operators of private prisons. The LED makes clear that the definition of a competent authority should only cover bodies which are not public authorities to the extent that they are entrusted by national laws to exercise public authority and public powers for law enforcement purposes. Competent authorities that are processing personal data for LEPs will also be processing data that is subject to the provisions of the GDPR (for example, human resource and procurement data) and, as such, this IA has attempted to monetise the costs attributable to the LED.

Members of the public benefit from increased rights over their personal data and the removal of the fee to exercise access to the data held about them. They also benefit from knowing that the new regime places greater responsibility on data controllers and processors to protect their data.

A.3 Consultation

Within Government

In developing the law enforcement policy positions there was no formal consultation or call for views run by the Home Office. This was a decision taken due to the specific sector specific nature of the LED. Discussions were held with a range of stakeholders at the Whitehall data protection network and workshops were run with law enforcement agencies.

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

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

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

B. Rationale

With the increase in the use and the advances in technology, data is being processed and transferred at increasing rates. An increase in the collection and sharing of personal data comes with the need for a stronger and more coherent framework for the protection of personal data. For international transfers the LED will replace the provisions set out in the 2008 Council Framework Decision on the protection of personal data processed for police and judicial co-operation in criminal matters. The 2008 Decision on international transfers was adopted into domestic legislation by Part 4 of the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014. The provisions of the Data Protection Bill transposing the LED into UK law will replace the relevant sections of the current DPA which was adopted following the EU Data Protection Directive 1995.

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 the barriers to data sharing that occur where different countries apply different standards of protection.

Without transposing the LED into domestic legislation the UK would risk infraction proceedings being brought against it by the EU. Not only will the failure to transpose the LED create a risk of infraction proceedings it will also negatively affect businesses and individuals as they try to apply the law effectively in a period of legal uncertainty. The importance of implementing the LED into domestic legislation goes beyond complying with the EU legislation whilst the UK remains a part of Europe. As highlighted in a recent report by the House of Lords EU Committee[4] "though the UK will not be bound by EU data protection laws post-Brexit, there is no prospect of a clean break. The legal controls placed by the EU on transfers of personal data outside its territory will apply when data is transferred from the EU to the UK." The cross-border flow of data is a critical requirement for effective police and judicial cooperation across national boundaries. The UK participates in a range of EU platforms for the sharing of data between law enforcement agencies which are based on shared standards of data protection and are vital for UK law enforcement agencies. In implementing the LED into domestic legislation now, the UK's ability to continue to share personal data after the exit from the EU will be strengthened for law enforcement purposes.

C. Objectives

In transposing the LED into domestic legislation it is intended to keep the UK in step with the levels of data protection being applied across the EU. In doing so those members of the public who have their personal data processed for law enforcement purposes know that they have increased rights and protections around their data. Annex C contains a summary of the data protection requirements introduced by the LED. Data controllers will need to consider data protection by design and default in creating new methods of data processing. This is coupled with data controllers having to put in place robust processes to ensure compliance whilst increasing the role of the independent regulator, the ICO. Through these steps it is intended that there will continue to be the free and unhindered flow of data for police and judicial co-operation between the UK and the rest of the EU. Post the UK's exit from the EU the successful transposition and implementation of the LED into domestic legislation will help to ensure that the UK can obtain new arrangements to govern the continued free flow of personal data between the EU and the UK.

[4] House of Lords European Union Committee Report (2017) '*Brexit: the EU data protection package*'; 3rd report of session 2017-19; Paragraph 2: https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/702.htm

D. Options

Option 1 is to make no changes (do nothing).

Currently domestic personal data processing for LEPs is governed by the DPA and international transfers are governed by the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014. When the EU data protection package comes into force in May 2018 they will form a new EU framework for data protection which will provide stronger data protection than the current UK regime. The do nothing option is to retain the current domestic legislation for law enforcement personal data processing. This option carries significant risks. Individuals, businesses and public bodies would face increased complexity and uncertainty which would hinder the effective application of data protection legislation and cross-border cooperation. Although EU directives are not directly applicable to a domestic court in the same way as a regulation, a court can still consider them and apply their provisions when a country fails to correctly transpose the contents into domestic legislation (subject to the applicable legal test). Therefore, a failure to transpose the LED may not prevent law enforcement bodies being bound by the directive whilst the UK remains a member of the EU. However, the UK would face the risk of infraction proceedings from the EU and would have greater difficulty in continuing to share personal data for law enforcement purposes with EU Member States after the UK leaves the EU.

Option 2 is to implement the LED using domestic legislation.

Primary legislation will be enacted to transpose the LED into UK law and to replace the existing data protection legislation. In taking this approach there will be greater legal clarity than in Option 1 and the UK data protection regime for law enforcement purposes will be aligned with the rest of the EU. The LED seeks to build a strong framework for the protection of personal data that takes into account advances in technology. By transposing the LED into domestic legislation it can be introduced in a way that ensures the operational needs of UK law enforcement agencies are taken into account. Further, it will help the UK obtain new arrangements to govern the continued free flow of personal data between the EU and the UK once the country leaves the EU.

E. Appraisal (Costs and Benefits) of Option 2

GENERAL ASSUMPTIONS & DATA

Data and Assumptions

- There was no data on which to base any estimates of the impact of the LED. The Home Office therefore collected data through a survey[5] sent out to a sample of 88[6] out of an estimated 400 to 500 competent authorities believed to be in scope.
- Responses were received from 44 organisations, a response rate of 50%.
- Of the 44 who replied, 8 did not consider themselves in scope of the directive and 36 provided full responses to the questionnaire. However, some of these responses are consolidated returns, answering on behalf of a number of smaller agencies and private sector businesses.
- The consolidated returns could not be disaggregated, so have been counted as a single business. This should not bias results, as data were used to produce averages that were applied to estimates of the wider population.
- It is assumed that the sample responses are representative of the wider population of 'competent authorities'. This is a strong assumption as no responses were received from local authorities, who are expected to make up around half of all competent authorities and may operate significantly differently from those for which data is available. The Department for

[5] The full survey can be found in Annex D.

[6] Of which some have the ability to respond on behalf of numerous alternative organisations. For example the National Police Chiefs Council responded on behalf of all 43 police forces in England and Wales.

Communities and Local Government (DCLG) have stated that the LED will not disproportionately affect local authorities.

- There are limited returns from private sector bodies but the impact on some will be captured in consolidated returns. Because these consolidated returns could not be disaggregated the current assumption is that there is no difference between costs to the private and public sector.
- Local authorities generally have a more limited role as law enforcement agencies than the authorities in our sample. For this reason it may be expected that local authorities experience less of an impact, which suggests that the analysis may overestimate the burden of the policy.
- For all monetised estimates a social discount rate of 3.5 per cent is used to obtain present values, see HM Treasury (2003) Green Book[7]. Any estimate quoted (PV) or the Net Present Value (NPV) is discounted using this rate. The appraisal is over a ten year period.
- Sensitivity analysis was conducted around the wider scale of the impact, the cost to authorities of becoming compliant, the change in volumes of subject access requests following the removal of fees and the burden of producing data protection impact assessments on both the authorities and the independent regulator. All of these analyses are presented in section F.

Scale

- The LED applies to competent authorities who process personal data for law enforcement purposes.
- About 400 competent authorities were identified as 'in scope': including 240 local authorities, over 45 police forces, 31 rail and tramway franchises, and 80 to 100 central government departments and agencies.
- Of the 400, 34 private sector businesses are identified as being within the scope of the LED, but there will be more when taking into account handling services contracted out from public sector agencies to the private sector that are data controllers. Around half of survey respondents stated they contract services to the private sector; however, it is not possible to verify whether these businesses are in scope without looking into their specific legal arrangements. This is because many private businesses may be data processors and not controllers and thus would not qualify as competent authorities.
- The best estimate uses an assumption based on indications from those working with the sector, that of those who contract out (200), 25% do so with data controller roles, bringing 50 more businesses into scope. This gives a final estimate of the total number of agencies in scope of 450.
- The best estimate of the number of private sector businesses falling in scope of the legislation is 84 (34 identified and an estimated 50 more), however there is a degree of uncertainty around this. There is no central record of the number of private bodies who undertake personal data processing, as a data controller, for law enforcement purposes that is based upon a statutory function. Commercial contracts will need to be reviewed to determine if a private body that is processing personal data for a criminal law enforcement purpose, where public power or authority is given by statute, in order to determine if they are a controller or a processor. This will determine if they are a competent authority or not. Competent authorities will need to take into account policy and legal advice that is specific to their law enforcement data processing and apply a risk based approach to compliance.

- Prior to the introduction of the Bill, competent authorities referred to uncertainty around how the LED and the GDPR were going to be implemented into domestic legislation as one reason as to why it has been difficult to provide costs. This, coupled with the need for guidance and interpretation, has added layers of difficulty. The EU are still working on draft guidance, as are the ICO, for the LED which once published, will assist organisations perform the required compliance assessments. The Bill is designed to create new standards for data protection in the UK that will remain in force once the UK exits the EU. There are however, significant

[7] HM Treasury (2003) The Green Book, Appraisal and Evaluation in Central Government, (2003 version includes amendments made in July 2011), London. See: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220541/green_book_complete.pdf

benefits that have not been monetised around having the EU data protection standards in place after the UK leaves the EU.

OPTION 2 – Implement the LED using domestic legislation

As discussed in section D of this IA Option 2 is to transpose the LED into primary legislation in such a way that best meets the needs of the UK. It is this option that is appraised below against a baseline of 'do nothing.' The 'do nothing' option creates legal uncertainty, it creates the prospect of the UK courts finding parts of the LED being applicable whilst the UK is a member of the EU and it would risk the UK's future ability to share relevant personal data with EU Member States.

Costs

As discussed above, the large majority of the impact of this policy falls to public sector agencies and separate private sector estimates could not be produced. Unless specified, all costs listed below are averages that apply to public and private sector law enforcement agencies.

All competent authorities that would process personal data for law enforcement purposes will also process personal data under the GDPR (such as employee data for human resources). Although the economic impact questionnaire asked specifically about the costs and benefits related to the LED in the questionnaire, it is likely that some estimated costs may over-state the actual cost due to synergies between the GDPR and the LED. The analysis is focussed on the costs associated with the LED.

Compliance costs

Each agency and business impacted by the LED will incur costs from complying with it. These might include the need to upgrade the security, functionality and features available in their data processing systems. For example, the LED requires that systems allow for the marking out of data that is based on fact from data that is based on a personal assessment.

The costs of compliance will depend on an organisation's current level of compliance with the DPA. The majority (97%) of respondents indicated they were not currently compliant with the requirements set out in the LED and stated that they are currently unable to estimate the costs involved with becoming compliant. Competent authorities will need to make risk based judgments about establishing compliant data processing systems. They will need to analyse all the strands of personal data processing that they carry out and determine the legal basis upon which data is processed and from this if the process would need to meet the requirements of the GDPR or the LED. There is no uniform roadmap for making systems compliant with the LED. The data that has been collected highlights the difficulties currently faced by businesses in mapping out their current processes and systems in order to conduct a gap analysis.

The survey asked about the monetised costs of getting systems up to the required standard. However, only one agency provided monetised costs of compliance. This reflects the difficulty faced by competent authorities in estimating the costs of compliance. As stated above, the costs of compliance will depend on an organisations current level of compliance and the results of a detailed mapping exercise in order to identify the requirements to meet the LED. At this time such costs are not available and would require disproportionate effort to be estimated. This figure, together with the non-monetised responses, is used to estimate the impact on agencies and business that responded to the survey. These estimates are then scaled up to all agencies/businesses thought to be impacted by the LED. This gives an estimate of one-off costs of £29.9 million in total, including £5.5 million to private sector businesses from compliance with the LED.

These costs can be realised at the discretion of the authority at any time up to 10 years after the introduction of the LED; assuming the costs are spread evenly over the next ten years gives a present value cost of £25.7 million. Further information is available in Annex E.

The estimates make the strong assumption that the compliance costs from one agency are representative for all agencies where a cost is incurred.

Subject Access Requests (SARs)

SAR fee income

The LED removes the right of authorities to charge for SARs (except in exceptional circumstances), so authorities that currently charge will lose revenue.

The survey reveals which authorities charge for SARs, how much they charge, and how much it costs them to process the fee.

The estimated average cost of £1,400 per authority per year does not apply to all 450 authorities equally. This is because half of authorities (225) do not currently charge for SARs so will experience no negative impact. The impact on the 36 per cent who do charge and will have to stop, is estimated at around £3,200 per authority per year[8].

The estimated average cost of £1,400 per authority per year does is multiplied by the 450 authorities to give the total impact. This is estimated to be around £0.6m per year. Sensitivity analysis was conducted around this, and can be seen in section F.

Because the fees for SARs are paid by cheque, the cost of processing the payment can be very high and anecdotal evidence suggests that it can often exceed the value of the cheque itself, so the fee (currently capped at £10) exists to serve as a deterrent against vexatious requests.

The cost of processing cheques is based on an average figure constructed from the three responses from those who charged a fee and gave monetised cost estimates. The average figure is applied to all authorities that charge for SARs and did not give a monetised estimate of their processing cost.

The full breakdown of the lost SAR revenue can be seen in Annex F and is calculated as follows:

Number of SARs x (fee charged - processing cost per SAR)

This estimate rests on the following assumptions:

- Fees are always collected.
- Where no cheque processing fee is supplied, the average of those that provided a response is used (that is, there is no bias in which firms chose to give monetised estimates).
- Where respondents gave processing fees of 'up to £10', an estimate of £8 was used.

Volume impact of SAR fee removal

As mentioned above, authorities charge fees for SARs as a deterrent against vexatious requests, because the cost of fulfilling SARs (costs relating to the time and resources needed to prepare a response along with the cost of administering the fee) is often significantly higher than the fee, which is capped at £10. If this deterrent is removed there is likely to be an increase in applications to businesses that currently charge a fee. This cost was calculated by assessing the average cost of fulfilling a SAR.

The cost of fulfilling SARs varies considerably between agencies because of differences in the complexity, volume, and age of the data they hold on individuals. Of the authorities who charge for SARs, the quantified volume received and fulfilment cost estimates from 13 different authorities,

[8] Around 14 per cent didn't know their policy on SARs, so no estimate could be calculated.

allow authority-specific costs per SAR to be estimated[9]. The average cost of fulfilling a SAR is £225. This is applied to the relevant authorities that gave volume but not cost estimates.

The survey asked about the expected cost increase of a rise in volumes following the removal of the SAR fee, we received two responses that quantified their anticipated additional cost, but none that estimated the extent of the increase. Respondents provided a number of qualitative responses as to whether or not they anticipated any increase in the number of SARs. Given the difficulties associated with estimating an unknown future impact and the scale of these costs in relation to the IA as a whole, it would require a disproportionate effort from survey respondents to provide meaningful cost estimates at this time. The qualitative responses gave a broad indication of the size of the increase. Where agencies expected a small or medium increase in the volume of SARs, but do not quantify it, an assumption of 5 per cent was used. Where agencies expect a large increase in the volume of SARs, but do not quantify it, an assumption of a 10 per cent increase was used. These assumptions are tested in Section F using sensitivity analysis.

SAR volume estimates were multiplied by the relevant increase to give the anticipated change in volumes, which was then multiplied by the cost per SAR for that business. The average cost of the increased volume is estimated at £11,300 to each of the 450 authorities. This includes about 36 per cent of authorities who are not affected at all (as they did not charge for SARs in the first place, or expected no increase) and a 33 per cent who are affected[10]. The average impact on affected authorities is £23,500. In exceptional circumstances the Bill will allow competent authorities to charge a fee to cover reasonable administrative costs or to refuse to action manifestly unfounded or vexatious SARs.

The average cost of the increased volume is estimated at £11,300 to each of the 450 authorities therefore the total annual impact is expected to be around £5.1 million.

Costs of Data Protection Impact Assessments

The LED requires competent authorities to produce Data Protection Impact Assessments (DPIAs) when making changes to their systems. This represents an increase in work and therefore a cost to authorities.

The survey asked for a cost estimate of the need to produce DPIAs, to which 16 respondents stated '*there would be no additional cost as they already produce DPIAs*.' Ten did not quantify the cost but expected it to be low (additional work for some employees, but no significant expenditure), four anticipated a higher cost (of which one response suggested a single additional FTE), and six did not provide an answer.

Where authorities suggested there would be a high cost, this assumed an additional burden of one FTE at a rate of £25,000 per year. Where agencies suggest there will be a low or medium cost, the assumption of the additional cost equated to a half FTE at the same rate. As many suggested that there would be no additional expenditure, it should be noted that these burdens can represent the opportunity cost of employees spending time on DPIAs, rather than other productive activities.

As before there is a distinction between the costs that fall to authorities that currently do or do not conduct DPIAs. Approximately 44 per cent of authorities are estimated to face no additional cost, and 39 per cent face an additional cost and there was insufficient data on the remaining 17 per cent. The average cost to those authorities affected is around £16,000 per year. The estimated average cost is £7,500 per authority per year, giving a total cost to all 450 authorities of around £3.4 million per year[11].

[9] These can be seen in Annex F.

[10] A further 30% did not provide enough information to allow estimation.

[11] Full details can be seen in Annex G.

Familiarisation costs

There may be some familiarisation costs in relation to the new rights of data subjects and the applicable exemptions contained in the LED. The familiarisation costs have been estimated by asking a sample of competent authorities how many employees would require specific training on the LED and how long this training/guidance will be. Out of 14 responses, 12 replied with estimates on the number of staff requiring training and 4 responded with an estimate of the length of the guidance. These estimates suggest the average number of employees requiring specific LED training at around 50 with the average length of the training/guidance being approximately 2,400 words.

To estimate the total amount of time employees in competent authorities may spend familiarising themselves with the LED the number of employees are multiplied by the estimated length of the training guidance. These are then used alongside the standard reading tables (see Table 1) to estimate the total amount of time employees spend on familiarisation of the LED. In instances where the competent authority did not provide an estimate the averages for the number of employees and the length of the training/guidance were used.

Table 1: Reading speed assumptions

	Speed (wpm)	Comprehension
High	100 (slow)	50%
Central	200 (average)	60%
Low	400 (good)	80%

The assumption for reading the guidance/training (2,400 words on average) for the additional question is taken to be 6, 12 and 24 minutes for the low, central and high scenarios. The reading times were estimated using standard tables from readingsoft.com[12] (see above). Because of lower comprehension a slow reader may need to re-read the guidance. For example, it is assumed a slow reader will need to re-read half the document again to fully understand it whereas a good reader will only have to re-read 20 per cent of the document.

The total amount of time spent reading the document is then multiplied by the average wage to estimate the total familiarisation costs. The responses to the survey suggest the guidance would need to be read by employees ranging from Executive Officers to the Senior Civil Service. It was not possible to construct a reliable distribution. We have therefore assumed the salary of a Home Office Higher Executive Officer (HEO) including employer NI contributions and employer pension contributions (gross wage per hour= £27.66). Using the low, central and high reading speeds and total volume of competent authorities (450) the familiarisation costs range from approximately £70,000 to £420,000 with a central estimate of £180,000. These costs are assumed to apply only in year 1 of the policy.

There may be other familiarisation costs. Examples include if systems are replaced or upgraded and user interfaces change as a result of new requirements or where there are new requirements to demonstrate compliance and culturally adapt to a system where data protection by design will be a key part of data processing system creation. However, this is uncertain in all cases and it would be very difficult to estimate the extent of the change, numbers of people affected, or to separate the specific costs out from those that would take place along with any other planned system update or upgrade. . A question was asked on whether competent authorities could estimate these costs, however all suggested they could not estimate the associated costs at this time.

Costs to the Independent Regulator

The Information Commissioner's Office (ICO) enforces data protection legislation, so are impacted by the LED, during a consultation they identified four main ways in which ICO will be affected by the directive:

[12] Readingsoft is a website that provides information on reading speeds and comprehension see http://www.readingsoft.com/

1. Increased awareness of breaches;
2. Increased consultation around DPIAs;
3. Increased use of sanctions;
4. Increased numbers of complaints.

All of these were monetised except the increased number of complaints, giving a total annual cost to the ICO of £0.6 million.

1. Increased awareness of breaches

The LED includes new requirements of mandatory breach reporting, which ICO expect to lead to a 50 per cent increase in their awareness of both minor and major breaches[13].

In 2016/17 the ICO received 2,565 self-reported incidents under the DPA including private sector and public sector[14]. Of these, 125 (5%) related to the Police and Criminal Justice sectors. The ICO assume that the new requirements for mandatory breach reporting will result in a 50 per cent increase in reporting. This is based on sector specific knowledge and assumed current under-reporting. Therefore, we can expect a revised figure of around 250 incidents in this sector post-implementation.

The ICO assumes that after initial sorting of the breaches, between 10 per cent and 20 per cent of the remaining cases would need investigating. The cost of investigating cases in this area can vary considerably. However, ICO estimate that a total increase of £500,000 per annum would be a realistic estimate.

2. Increased consultation around DPIAs

DPIAs will draw attention to risks and problems with proposed changes to systems or procedures. Where the supervisory authority is of the opinion that risk persists, specifically as a result of data controllers' insufficient steps to identify or mitigate against it, the LED[15] provides for supervisory authorities to respond to any consultation with guidance to controllers within a specific timeframe. The ICO anticipate that this additional requirement will incur costs from having to consult with data controllers on how to best mitigate the risks highlighted by DPIAs. It is estimated that 20 per cent of all DPIAs conducted by the private, public and third sector will highlight substantial risks that will require consultation with the ICO, equating to around 7,000 DPIAs per year. The estimated cost per DPIA authorisation has been made at between £200 and £400 per consultation.

Based again on a figure of 5 per cent of the 7,000 relating to the Police and Criminal Justice sector the ICO could receive 350 DPIAs relating to the LED at a cost of between £70,000 and £140,000 per year. For the central estimate it is assumed the mid-point (£105,000) to be the most representative cost. There is sensitivity analysis around the ICO estimate in Section F.

3. Increased use of sanctions

The scope of sanctions under the new regulatory framework is wider than under the current DPA and as such it is likely that the ICO will see an increased use of these sanctions.

The ICO previously projected that the Directive would result in up to 250 incidents investigated by the ICO. Based on the current proportion of investigations that result in a monetary penalty, the estimate assumes that around 1 per cent of concluded investigations will result in a financial sanction.

[13] Note this does not conflict with the monetised benefit, as that represents the value to society of the decreased risk of breaches occurring, not the cost to the regulator of investigating them. The anticipated outcome is better awareness of breaches (which comes at a cost to the ICO) but also fewer breaches overall (which has a benefit to society).

[14] Data Protection reports and concerns 2016/2017 https://ico.org.uk/about-the-ico/our-information/annual-operational-reports-201617/data-protection-reports-and-concerns/

[15] Article 28(5)

Therefore around three incidents relating to processing under the Directive are likely to attract a financial sanction within the first year of the Directive taking effect. As outlined previously, the cost per case in this area can vary considerably, however it is estimated that a total increase of £6,000 would be a reasonable estimate in relation to the cost to the ICO of issuing monetary penalties under the directive.

4. Complaints

The LED introduces new and enhanced rights for individuals and it is anticipated that the ICO will therefore see an increase in complaints from individuals. In 2016/17 the ICO received 18,354 complaints of which 917 related to the Police and Criminal Justice sector (not including courts or prisons) - 5 per cent of the total complaints received[16].

While the ICO do anticipate an increase in complaints under the new regulatory framework, uncertainty at the time of requesting responses on the scope of the LED (in relation to the definition of a competent authority) meant that the ICO were not in a position to assess what this may mean for this sector and the cost could not be monetised.

Total cost

Ongoing costs:

Lost SAR revenue:	£ 0.6 million
Increased SAR volumes:	£ 5.1 million
Cost of producing DPIAs:	£ 3.4 million
Costs to ICO:	£ 0.6 million
Total	**£ 9.7 million**

One-off costs:

Compliance costs:	£ 24.0 million
Costs of Features:	£ 5.9 million
Familiarisation Costs:	£ 0.2 million
Total:	**£ 30.1 million**
10 year annual average:	£ 3.0 million

Total costs:

10 year annual total:	**£ 12.7 million**
10 Year present value:	**£109.0 million**

Other non-monetised costs

Public sector bodies and private business could incur additional costs from having to update their methods of handling paper files; meeting additional requirements for data sharing; adjusting to shorter response times for SARs; expected increase in complaints about SARs; upgrading to prevent unauthorised processing of data; and the cost of increased numbers of complaints to the ICO. All of these were discussed in the commission letter, but there were no quantified responses to this question.

Cost of handling paper files

Question 8 in the survey asked about changes in the cost of handling paper files. The LED provisions apply to both automated and manual processing so that the protections afforded are

[16] Data Protection reports and concerns 2016/2017 https://ico.org.uk/about-the-ico/our-information/annual-operational-reports-201617/data-protection-reports-and-concerns/

technologically neutral and avoid the risk of circumvention. In this regard costs will be incurred in ensuring paper records that form part of a filing system meet the relevant standards such as categorising data subjects, distinguishing fact from personal assessment, have appropriate security and utilise the concepts of data protection by design and default.

Of the 36 respondents, 39 per cent stated no cost would be incurred, 19 per cent suggested that there may be a low, uncertain cost or minor disruption, and 14 per cent expected a higher cost. No respondent gave a quantified estimate of cost or scale, so this could not be monetised.

Additional requirements for data sharing

Question 10 asked for the costs or benefits associated with LED provisions relating to the transfer of data across borders. The LED provisions for international transfers are similar to those found in the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014 and as such for a number of competent authorities there would be no significant difference. However, the definition of competent authority was narrower in the 2014 Regulations than the LED. As such, there may be some bodies who will now incur cost to meet these provisions. Fifty-six per cent of respondents did not provide an answer to question 10, but 28 per cent indicated there would be no impact, 14 per cent were uncertain or thought there may be a minor impact and 3 per cent simply noted there would be additional costs.

Again, there were no quantified estimates and it was not possible to monetise the cost.

Change in response time for SARs

The LED requires that SARs be responded to without undue delay, which has been translated in the Bill as to being within one month. Question 15 asked about the current processing time of SARs and question 20 asked about the cost of the new time limit rules.

The responses to question 15 showed that 42 per cent or respondents already process SARs in 30 days or less on average, and 33 per cent have average processing times between 30 and 40 days[17].

No respondent gave any quantified cost (as asked at question 20[18]) of a rule requiring SARs to be processed in 30 days (+2 months) Of the responses, 8 per cent stated it would likely raise costs, 25 per cent were unsure or expected the burden would be minor, 31 per cent said there would be no change., Thirty-six per cent did not respond.

Although 42 per cent of respondents already process SARs in less than 30 days, some still anticipated minor costs from a reduction in the required processing time, this may be because there is variation around an average that remains less than 30 days and some SARs are very fast and others take much longer than 30 days.

Change in complaints about SARs

As a result of the compressed response requirement and increased volumes it is expected that the number of complaints may increase. Of the respondents 22 per cent indicated there would be an increase in complaints, 11 per cent were unsure or anticipated any increase would be small, 36 per cent expected no impact on the number of complaints. Thirty-one per cent didn't answer. This could not be quantified because there is no data on current volumes or costs of handling complaints.

[17] A further 22 per cent didn't answer the question, and 1 respondent (3%) had an average time of 37 days in 2016-17, but an average of 28 in the first half of 2017-18.

[18] Q 20: Would the reduction in processing time to within one month (plus two) result in any extra cost for your organisation? If so, can you estimate at what cost?

Upgrading to prevent unauthorised processing of data

There is a requirement that systems be robust to stop the unauthorised processing of data, which could come at a cost to those that will need to make changes to their systems. This is part of the requirement that the security around processing is commensurate to the risk and that appropriate technical and organisational measures are in place to ensure the appropriate level of security. Of those sampled, no respondent expected an additional cost, 8 per cent were uncertain about the impacts, 89 per cent were sure there would be no cost. Three per cent did not respond.

BENEFITS

SAR fee removal

By removing the fee for SARs, currently capped at £10, the revenue is transferred from the competent authorities back to the applicants.

This is calculated by simply multiplying the current SAR fees charged by competent authorities by the volume of SARs they receive. This is then scaled by the estimated number of competent authorities to give an estimated annual benefit of £1.5 million. As well as shifting money from authorities to applicants there is also a net gain to society, as much of the fee is currently lost to cheque processing, so cannot be used by the authority or the applicant. The total cost of cheque processing is estimated at £860,000 per year - all of which is returned to applicants through the removal of the fee. Previous[19] expert knowledge evidence, from those working with the sector, suggests some businesses may pay more than £10 to process each cheque, in which case this represents a cash saving to them too by removing both the fee revenue and the (larger), processing cost[20].

Reduced risk of breaches

The average fine issued by the ICO to law enforcement agencies is used as a proxy for the cost of a serious data breach. Fines issued by the ICO are varied to reflect the severity of the breach, but they may still underestimate the distress caused to individuals, reputational damage and other costs to society. The ICO provided data on all fines issued to competent authorities over the past five years, for which the average amount was £138,500 per year.

Consultation with the ICO suggested they expect to issue fines for three serious data breaches per year from competent authorities following the introduction of the LED, meaning the baseline cost is 3 x £138,500 = £415,500 per year.

Question 34 asked if respondents expect the LED to reduce the number of data breaches in their organisation. Exactly half of respondents expected no change in the number of breaches, either because they never suffered a breach or are already compliant with the LED, and 11 per cent of respondents stated that becoming compliant with the LED would reduce the risks of suffering breaches. The remaining 39 per cent did not respond to this question.

It is assumed that those who do expect an improvement become very unlikely to suffer a breach immediately after the introduction of the LED, therefore the expected number of breaches was adjusted down by 11 per cent, 3 x (1 - 0.11) = 2.67.

The new anticipated cost of breaches per year is then estimated as: 2.67 x £138,500 = £370,000. Subtracting from the baseline gives an annual benefit of £45,500 (£415,500 - £370,000).

[19] Page 7; 'SAR Fee Income'

[20] This is only a saving overall if the business is: i) paying more than £10 to process each cheque and ii) sees no volume increase following the removal of the fee.

Benefits to Business

The only monetised benefit to business is their share of the avoidance of the cost of serious breaches. Private sector businesses are estimated to represent around 19 per cent of the total number of competent authorities. It is assumed they are no more or less likely to suffer serious data breaches than the public sector, so this proportion of the total benefit is attributable to the private sector. This gives and annual figure of around £9,000, and a present value total of £74,000 (PV) over ten years.

Total Benefits

Annual Benefits:

Fewer breaches:	£ 0.05 million
SAR revenue to applicants	£ 1.5 million
Annual total:	**£ 1.5 million**
10 Year present value:	£13.0 million

Note: Figures do not sum due to rounding but the total is £1.5 million.

Non-monetised benefits

The main non-monetised benefits from this policy change are the ability to facilitate and maintain smooth sharing of LE data with the EU and its Member States as well as the enhanced rights and protections for members of the public whose personal data is held by a law enforcement agency. If this did not go ahead it would be significantly less likely that the UK law enforcement agencies would be found to have a level of data protection that would be in line with the European standard. The failure to get new arrangements to govern the continued free flow of personal data between the EU and the UK once the country leaves the EU will result in competent authorities having to make alternative arrangements with an increased cost through time and effort, lawyers and interpreters.

By implementing this policy, data protection regimes will be the same across the EU and it is anticipated that there will be harmonisation benefits, less fragmentation of different data protection regimes across the EU which will assist in judicial and police co-operation and cross-border transfers.

The LED provisions provide for enhanced levels of protection to personal data which should ultimately lower the total number of breaches that occur – including smaller scale breaches that do not illicit fines from the regulator. This increased level of protection will mean that data subjects can exercise greater control over the way their data is used with greater confidence that their data is safe. This should also mean a reduction in the associated costs that occur when data is lost - that being a reduction in the harm caused through less total breaches but also through better mitigation of the risks associated with breaches.

Business Impact Target, NPV, BNPV and EANDCB

The Business Net Present Value and Estimated Annual Net Direct Cost to Business are presented below but because the competent authorities are exercising public authority or public powers such as acting as a public prosecutor when pursing a criminal charge against a defendant then these costs are not defined as falling to a private sector firm. They are out with the scope of the Small Business, Enterprise and Employment Act 2015. As such these figures, although reported here in the evidence base, are not reported on the front two pages of the IA as a cost to business.

Net Present Value (NPV)

The NPV is estimated at -£96.0 million over ten years.

Business Net Present Value (BNPV)
The BNPV is estimated at -£19.4 million, which is calculated assuming the cost to each business is the same in all areas as the cost to each public sector body.
Estimated annual net direct cost to business (EANDCB)
The EANDCB is estimated to be -£2.3 million per year.

F. Risks

OPTION 2 – Implement the LED using domestic legislation

The risks associated with the preferred option of transposing the LED into domestic law can be split up into three parts. The first is in relation to the implementation of the LED provisions, the second is around the actual impact of the LED provisions, and thirdly that the costs and benefits may not be accurately calculated.

Implementation

In terms of transposing the LED into domestic legislation it is important that this is done faithfully to meet the intentions of the Directive whilst ensuring the needs of law enforcement agencies are taken into account. The risk here is that the provisions in the Bill as drafted do not meet the requirements of the LED and as such do not provide the right level of protection to data subjects. As a result of this there would be reputational damage to the Government and people may lose trust instead of gaining it regarding the security of their personal information. Additionally, this could lead to the UK not succeeding in obtaining new arrangements to govern the continued free flow of personal data between the EU and the UK once the country leaves the EU. The trade-off of the LED provisions is the Bill gives stronger data protection rights to individuals whilst demanding additional processing requirements of law enforcement operations, with restrictions to the data subject rights, when necessary and proportionate to protect the purpose of processing. In order to understand the balance required, work has been carried out with law enforcement agencies as well as regular attendance at the EU expert working group in Brussels. The LED provisions have been drafted for inclusion in the Bill and shared with stakeholders to ensure that the correct balance is struck.

Impact of LED provisions

The second risk is that the additional number of requirements under the LED provisions within the Bill will lead to an increase in the total number of breaches instead of a reduction. Having more rules may lead to it being more likely that someone will fail to comply with them. This would then lead to a reduction in the reputation of non-compliant competent authorities. The ICO anticipate that given the new requirements for stronger controls around compliance and the reporting of breaches that they will see a rise in the number of breaches being reported to them although the total number of breaches occurring would fall. The ICO are working with the Home Office on guidance that will assist competent authorities implement the LED correctly.

Economic analysis

The last risk is around the economic analysis of the impact of the LED on UK competent authorities. This is examined in the following section dealing with the sensitivity analysis that has been conducted. A full summary of the figures can be found in Annex H.

Sensitivity Analysis

In an attempt to test the robustness and convey uncertainty around estimates and assumptions, sensitivity analysis examines the effect of variations in the assumptions used in the cost estimates.

For the sensitivity analysis low, central and high scenarios were developed, varying the overall scale estimate; the cost to authorities of becoming compliant; the change in volumes of subject

access requests; and the burden of producing data protection impact assessments on both the authorities and the independent regulator.

Scale

As explained above, around 400 public and private sector authorities were identified as being in scope of the directive. However, although there are details of which authorities contract work to the private sector, without going into the details of each arrangement it is not possible to assess whether they are contracted as a data processor or a data controller. If the latter they would be a competent authority for the purposes of the LED.

The high estimate assumes that of the competent authorities that outsource to the private sector (200), half of these contract a data controller role to one private sector body that is entrusted by law to perform a public function, bringing around 100 additional private sector entities into scope of the LED. The central estimate is that of the 200 who contract out, a quarter will have data controller roles, bringing around 50 more businesses in scope. The low scenario assumes all contracted roles are as data processors, so no more private sector bodies are brought into scope.

This gives estimates of the total number of agencies in scope of 400 in the low scenario, 450 in the central scenario, and 500 in the high cost scenario.

Cost of compliance

The estimated costs of compliance are based on very uncertain cost estimates. The total cost is assumed to be £100,000 for all organisations who indicated there would be a significant cost to them. The sample contains a diverse range of organisations varying considerably in scale, structure and complexity so it is difficult to obtain an accurate estimate of the total cost.

A wide sensitivity analysis was conducted, creating a low scenario where non-compliant businesses face a cost of £50,000 and a high scenario where the cost is £150,000. Taking account of the fact that many businesses are (or have plans to be) complaint already, this gave average costs in the low, central and high scenarios of £27,000, £53,000, and £80,000 respectively.

Within the cost of compliance estimate is the requirement for systems to have certain features, for example, systems must be able to allow for the marking out of different data subjects by class/group (witness, suspect or victim). An assumed cost of £30,000 per authority was used, and the sensitivity analysis indicated low and high scenarios estimated costs of £15,000 and £45,000 respectively.

These gave overall average cost estimates of £7,000 in the low scenario, £13,000 in the central and £20,000 in the high.

These system features and compliance costs were then combined and scaled by the varying scale estimates discussed above, to give total cost estimates of £13.3 million in the low scenario, £29.9 million in the central and £49.8 million in the high.

Of these estimates the impact on the private sector is estimated at £1.1 million in the low scenario, £5.6 million in the central and £13.4 million in the high.

A full breakdown can be seen in Annex E.

SAR volumes

Of the authorities that currently charge for SARs, none quantified an increase in volumes but many provided qualitative assessments. For those that expected small or medium increases in the volume we assumed a 5 per cent increase, and for those expecting a larger increase we assumed a 10 per cent rise in applications.

When conducting sensitivity analysis the assumptions around costs were not altered as this data was relatively good, however the volume increases are not based on any quantified evidence so it is crucial that these assumptions are tested.

There are still two estimates per scenario, as authorities expressed whether they expected to see small or larger increases. In the low scenario an assumption of 0 per cent and a 5 per cent rise is used, in the central 5 per cent and 10 per cent, and in the high a 10 per cent and 20 per cent increase.

This gives average costs across all authorities of £7,000 in the low scenario, £11,000 in the central and £17,000 in the high. When scaled up to all authorities in scope[21], this gives annual costs of £2.8 million in the low, £5.1 million in the central, and £8.5 million in the high estimate. A full breakdown is given in Annex E.

Data protection impact assessments

Where authorities suggested there would be a high cost to the requirement to produce DPIAs, the estimate assumes, that this entails an additional burden of one FTE at a rate of £25,000 per year. Where agencies suggest there will be a low or medium cost the assumption is the cost equates to half that of the high burden (£12,500).

As there is not a robust evidence base for this, sensitivity analysis was conducted and scenarios were produced in which those expecting a high cost spend the equivalent of half an FTE per year in the low scenario, one FTE in the central and two in the high.

Those expecting a small or medium cost are assumed to pay the equivalent of a quarter, half or one FTE at £25,000 per year.

It is estimated that the overall average cost is £3,750 per authority per year in the low scenario, £7,500 in the central and £15,000 in the high. As before, there is a distinction between the costs that fall to authorities that currently do or do not conduct DPIAs. Roughly 44 per cent of authorities will face no additional cost, and 39 per cent face any additional burden. The average burden to those who are affected is £8,000 per authority per year in the low scenario, £16,000 in the central and £32,000 in the high. Full details can be seen in Annex F.

When scaled up, again scaling the low cost by the low scale estimate and so on; these give total costs of £1.5 million in the low scenario, £3.4 million in the central and £7.5 million in the high scenario.

NPV, BNPV and EANDCB

The results of these sensitivity analyses were used to produce high, central and low estimates of the NPV, BNPV and EANDCB. These represent the extremes of the analysis as there has been no combination across scenarios, for example the low NPV represents the summation of every low estimate.

The high NPV is -£178 million, the central -£96 million, and the low is -£46 million (PV) over 10 years.

The high BNPV is -£50 million, the central -£19 million, and the low is -£4.5 million (PV) over 10 years.

The high EANDCB is -£5.8 million, the central -£2.3 million, and the low is -£0.5 million.

[21] Such that the low cost estimate is scaled by the low scale estimate, the mid-point by the mid-point, and so on.

Small and micro business assessment (SaMBA)

Under the Small Business Enterprise and Employment Act 2015, a small and micro business assessment (SaMBA) needs to be conducted. There is no sector specific evidence or a breakdown of private sector contractors or authorities by employment size band therefore the whole of this validation impact assessment acts as a SaMBA.
This lack of size band evidence meant that average costs had to be allocated equally across all authorities, however the most burdensome part of the directive relates to system readiness, compliance and features and SAR volumes. All of these costs are likely to be closely correlated with the scale and complexity of the authority in question. For this reason it is unlikely that small or micro businesses will face any unique or overly burdensome costs.

G. Enforcement

The LED builds upon the role of the ICO as the independent regulator. The provisions in the LED are compliant with the regulators code in that there will be a continued function for the ICO to assist individuals in exercising their rights. The LED further creates greater requirements for competent authorities to demonstrate compliance, report breaches and consult with the ICO adopting a risk based approach.

H. Summary and Recommendations

Table H.1 outlines the costs and benefits of the proposed changes.

Table H.1 Costs and Benefits		
Option	**Costs (£ million)**	**Benefits (£ million)**
1	£0 (PV over 10 years)	£0 (PV over 10 years)
2	**Ongoing costs** Lost SAR revenue £0.61 Increased SAR volumes £5.08 Cost of producing DPIAs £3.38 Costs to ICO £0.61 **Total £9.68**	**Annual Benefits** Fewer breaches £0.05 SAR revenue to applicants £1.47 **Total £1.52**
	One-off costs Compliance costs £24.00 Costs of Features £5.91 Familiarisation Costs £0.18 **Total** £30.08 **Annual** £3.01	
	Annual Total £12.70 **10 Year PV** £109.00	**10 Year PV** £13.00
	Public sector bodies and private businesses processing personal data under the LED could incur additional costs from having to update their methods of handling paper files, meeting additional requirements for data sharing, adjusting to shorter response times for SARs, expected increase in complaints about SARs, upgrading to prevent unauthorised processing of data, and the cost of increased numbers of complaints to the ICO.	The crucial non-monetised benefits of the LED are the ability to facilitate smooth sharing of LE data with the EU and its Member States, and the enhanced rights and protections for members of the public whose personal data is held by any law enforcement agency.

I. Implementation

The Government plans to implement these changes in line with requirements of the Directive so that the provisions come into force in May 2017.

J. Monitoring and Evaluation

This section shall be kept under review in line with the implementation and the use of powers by the ICO. In the normal way, the Data Protection Bill will be subject to post legislative review.

K. Feedback

Stakeholders have raised a number of issues that we are working through that will be reflected in the legislation to ensure the LED is transposed in a way that meets the operational needs of the competent authorities fulfilling their law enforcement functions.

Annex A

The differences between the Law Enforcement Directive (LED), the General Data Protection Regulations (GDPR) and the Data Protection Act 1998 (DPA)

A number of the main concepts and principles contained in the EU data protection package are similar to those found in the existing UK data protection legislation, however there a number of new requirements and enhancements. The Department for Digital, Culture, Media and Sport (DCMS) have produced an economic impact assessment looking at the costs and benefits of the permissible derogations within the General Data Protection Regulations (GDPR). The DCMS impact assessment contains a summary of the key changes introduced by the GDPR over the current Data Protection Act 1998 (DPA). These are:

- Data Protection Impact Assessments (DPIAs).
- Data Protection Officers ('DPOs').
- Demonstrating Administrative Compliance.
- Abolishing Notifications.
- Changes to the time limits and fees for Subject Access Requests ('SARs').
- Data Portability (DP).
- Right to Erasure.
- Data Breach Notification.
- Administrative Sanctions.

The LED generally follows the requirements found in the GDPR and sets out the protections to be put in place whilst taking into account the operational needs of law enforcement agencies. The main differences between the GDPR and the LED (other than the focus on law enforcement agencies) are:

- The LED does not contain provisions requiring processing to be transparent.
- The LED contains a requirement, where possible, to categorise data subjects by group that is, for example by witness, victim, suspect.
- Additionally, as far as possible, the LED requires data to be clearly distinguishable between what is a fact and what is a personal assessment. The LED also seeks, where practical, for steps to be taken to verify the quality of data before making transfers.
- The information that should be made available to a data subject (subject to permissible restrictions) is less onerous than under the GDPR.
- Under the LED a Member State may adopt provisions to restrict, wholly or partly, a data subjects rights (including erasure) under certain circumstances. The Bill seeks to utilise this key derogation just as it seeks to utilise the permissible restrictions allowed in the GDPR. The Bill gives competent authorities the power to neither confirm nor deny if information is held by allowing an individual's rights to be restricted in order to:
    a) Avoid obstructing official or legal inquiries, investigations or procedures.
    b) Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties.
    c) Protect public security.
    d) Protect national security.
    e) Protect the rights and freedoms of others.
- Data subjects in the LED do not have the same rights to object to processing as contained in the GDPR.
- The LED contains less EU oversight than the GDPR.
- The LED contains stronger requirements than the GDPR in order to demonstrate compliance, notably a logging requirement. Competent authorities will need to maintain logs of processing operations in automated processing systems around the collection, alteration, consultation, disclosure including transfers, combination and erasure of personal data (this could be the metadata that an automated processing system generates to record when data was entered, accessed and deleted and by whom).
- The LED also contains variations in the role of the Information Commissioner as the supervisory body.

Annex B

The interplay between the LED and the Investigatory Powers Act 2016

Once it is fully commenced, the Investigatory Powers Act 2016 will provide an updated framework for the use by the intelligence services, law enforcement and other public authorities of investigatory powers to obtain communications and communications data. These powers include the interception of communications, the retention and acquisition of communications data, and equipment interference for obtaining communications and other data. The Investigatory Powers Act also introduced enhanced world-leading oversight arrangements for the use of these powers.

By contrast, the LED does not provide a legal basis for obtaining communications or other data; instead it deals with the processing of personal data for law enforcement purposes ("processing" includes the collection, recording, organisation, structuring and storage of personal data).

Despite these differences, there is clearly some overlap between the LED and Investigatory Powers Act. Much of the communications and other information which will be obtained by law enforcement using the powers provided for in the Investigatory Powers Act will amount to "personal data" for the purposes of the Data Protection Bill. While the LED safeguards on processing will be relevant in this context for many public authorities, the Investigatory Powers Act also provides for additional explicit safeguards on the retention and disclosure (including disclosure overseas) of material obtained using the powers provided for in the Act. Furthermore, while the Information Commissioner has a leading oversight role under the Bill, they also have an oversight role under Part 4 of the Investigatory Powers Act regarding compliance with requirements and restrictions in relation to the integrity, security or destruction of communications data retained by telecommunications operators.

Under the LED personal data processing for any of the law enforcement principles needs to be lawful and fair. The LED requires processing to be in accordance with the law and can be based upon statutory powers, such as the powers in the Investigatory Powers Act, or consent.

The LED requires personal data to be only held for as long as it is needed to fulfil the law enforcement purpose that is required. Private and public bodies should have relevant review and retention periods for data that meet their operational needs. Both of these requirements are consistent with the additional safeguards provided for in the Investigatory Powers Act, applying to material obtained using the powers in that Act.

The Home Office have discussed the interplay between the Investigatory Powers Act and the LED with the ICO. The ICO has confirmed that to the extent that the reporting of breaches to the Investigatory Powers Commissioner (IPC) under the IPA might also require the reporting of a personal data breach to the ICO that this has been resolved in favour of the IPC. Potential dual reporting will not be required; any breach under the IPA should be reported to the IPC which is expected to inform the ICO in due course, where necessary.

Annex C

The new data protection requirements introduced by the LED

Overarching Title	Description	Government's Objective / Policy Position
LED Scope	The LED applies to the processing of personal data by competent authorities for law enforcement purposes both domestically and for cross-border transfers.	To apply the LED standards to all law enforcement agencies that meet the definition of a competent authority that process personal data for a law enforcement purpose (i.e. 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 (which is distinct from national security)).
LED System Readiness and Lawful Processing	In order to meet the requirements of the LED and the GDPR the processing of personal data must be lawful. It is a necessary precursor that those affected by the LED and the GDPR know the legal basis upon which they are processing data as this will identify whether that process is subject to the LED or the GDPR. If the purpose of the processing is for a LEP then there are system requirements to be met.	The key system requirement for LEP that does not appear in processing under the GDPR and the DPA is the requirement for logs to be kept of processing operations in automated processing systems capturing the collection, alteration, consultation, disclosure including transfers, combination and erasure. Qualitative evidence is that a well designed system should already capture meta data of when these functions occur. The requirement to log erasure does not require a competent authority to do more than log that a data subject's data has been deleted.
LED Principles	Included in the LED principles is the requirement for personal data, where applicable and as far as possible, to distinguish between the data of different categories of data subjects. Furthermore, there is a requirement, as far as possible, to distinguish between data that is based on facts from that which is based on personal assessments. In addition to this Competent Authorities must not transfer data without first taking	It is the Government's intention to implement the LED and the GDPR in a way that best supports the best interests of the UK. A data subject has the right to know that the data held about them is accurate and that they are able to rectify any inaccuracies.

	steps to try and confirm the accuracy of the personal data held.	
LED Rights of the Data subject	Chapter 3 of the LED sets out the rights of the data subject. The rights afforded to a data subject are not wholly different from those found in the DPA. The pre-existing rights and principles have been strengthened rather than created anew. An individual has the right to be provided with certain information (e.g. the identity and contact details of the data controller and the data protection officer, the purposes and legal basis of the processing, the data that is held relating to them, and the right to rectification or erasure). Individuals (natural persons) can make SARs to be provided with access to the data that is held regarding them, under the LED (and the GDPR) the data is to be provided free of charge except where a request is manifestly unfounded or excessive, in particular when repetitive in nature, a controller may either charge a reasonable fee (taking into account administrative costs) or refuse to act on the request.	In strengthening the rights of data subjects and removing the ability to charge for SARs an individual can have greater control over their data and how it is processed. The LED allows Member States to create provisions that restrict those rights. The Data Protection Bill will include provisions to allow law enforcement agencies to neither confirm nor deny that personal data is being processed to take account of their operational needs. The LED further stipulates that SARs should be responded to without undue delay, the current provisions allow up to 40 days to respond. The policy position is to mirror the timeframe under the GDPR (one month). Data Subjects who feel that a competent authority has not met their obligations under the LED can raise a complaint with the ICO.
Ability to Demonstrate LED Compliance	Ultimately one of the major differences in the application of the new Data Protection Regime is the stronger requirements for organisations that process personal data to be able to demonstrate compliance. Under the LED there is a need to log processing conducted by automated means. Furthermore there is a requirement that Data Protection Impact Assessments be conducted when changes to processes are being considered that are likely to result in a high risk to the rights and freedoms of natural persons and for the ICO to be consulted. The role of DPIAs is to help ensure appropriate mitigating actions	The ability to demonstrate compliance is a key requirement of both the LED and the GDPR. The ICO will have oversight of processing conducted under the LED and can request evidence to be provided to demonstrate a competent authority's compliance. One such piece of evidence is a log of processing done by automated means. It is intended to make use of a permissible derogation from the logging requirements that will allow automated processing systems set up before 6 May 2016, (exceptionally where it will involve disproportionate effort to be compliant with the logging requirement) to be brought into conformity by 6 May 2023 (with the possibility of a further three years if required).

	are put in place to respond to the identified risks. Competent Authorities should use DPIAs as a way to ensure **the principles of data protection by design and data protection by default** are met.	
LED Benefits	The LED is a part of a new comprehensive EU data protection package aimed at enhancing the coherence and consistency of EU data protection rules. The LED is the specific section of the package that will bring greater consistency to the field of police and judicial cooperation in criminal matters.	In transposing the LED into domestic legislation that we intend to create consistency in the personal data processing for law enforcement purposes of competent authorities. In doing so the Data Protection Bill will strengthen the rights of individuals and the control they can exercise over their own data subject to the operational restrictions required for law enforcement agencies. By implementing the LED the UK will continue to demonstrate its strong commitment to data protection and will operate a system more closely aligned with the rest of the EU in order to allow the unhindered sharing of information across-borders for law enforcement purposes.

Annex D

Law Enforcement Directive
Economic Impact Assessment Questions

LED Scope

1. Can you confirm that your organisation processes personal data that falls under the scope of the LED?
2. Do you consider any private body or entity that your organisation works with or have contracted/licensed with to work with personal data falling under the scope?
3. Can you provide any information that you have in relation to the costs/benefits/contract details/or named contacts within any relevant private body or entity that you work with that will fall under the scope of the LED?

LED System Readiness and Lawful Processing

4. Are your organisations systems already compliant with the LED requirements?
5. Has your organisation determined the legal basis upon which different processing is conducted (process mapping)? This will help determine whether the LED or GDPR is applicable.
6. If your organisation's systems are not compliant – do you have pre-existing plans to update/upgrade/replace processing systems to become compliant that you would have been implementing regardless of the new EU data protection legislation (i.e. plans to upgrade prior to May 2026)?
7. If your organisation is creating/implementing plans because of the LED in order to ensure compliance can you please outline what cost you think this will be?
8. Does your organisation have any paper files that will need to be treated differently as a result of the LED? If so, at what cost?
9. Do you share personal data with other EU countries? If so, how many?
10. Will the provisions in the LED around the transfer of data across borders lead to any increased costs or benefits from the current system? If so, how and to what extent?

LED Principles

11. Doe your organisations' systems currently allow for the marking out of different data subjects by class/group i.e. – witness, suspect, or victim?
12. Does your organisations' systems currently allow for the marking out of data that is based on fact from data that is based on a personal assessment?
13. Do your organisations' systems allow you to amend inaccurate personal data and to inform the Competent Authority where it originated from as well as notifying any recipients?
14. If the answer to any of the last 3 questions is a 'no' can you outline any steps being taken or contemplated to have these functions along with an estimate of the cost to your organisation?

LED Rights of the Data Subject

15. What is the current average response time within your organisation for law enforcement SARs?
16. What is your organisations current volume of law enforcement related SARs?
17. Does your organisation currently charge for law enforcement related SARs? If so, is this £10 or a lower amount?
18. If applicable, can you estimate how much it costs your organisation to process the cheque (SAR fee)?
19. How much does your organisation spend in order to respond to law enforcement related SARS (excluding the cheque processing fee)?
20. Would the reduction in processing time to within one month (plus two) result in any extra cost for your organisation? If so, can you estimate at what cost?
21. Does your organisation anticipate any change on levels of SARs received in light of the LED? If so can you estimate at what cost?
22. Does your organisation anticipate any change to the level of complaints received against SAR responses? If so can you estimate at what cost?

Ability to demonstrate LED compliance

23. Do your systems already meet the logging requirements? If not what plans are in place and at what cost to meet this requirement?
24. There is a derogation in the LED that if to become compliant by 6 May 2018 would require "disproportionate effort" the logging requirement for systems set up before 6 May 2016 can be extended to 6 May 2023. If you plan to rely on this would your system 'upgrades' taken place as a matter of course regardless of the LED requirement?
25. The LED lays out requirements for Data Protection Impact Assessments to be conducted when changes to processes are being considered that are likely to result in a high risk to the rights and freedoms of natural persons and for the ICO to be consulted – will this lead to further costs to your organisation? Can you estimate what these are?
26. Does your organisation currently have adequate security measures to stop unauthorised processing, to be able to restore data, to maintain reliability and integrity? If not do you have plans in place to meet these requirements and at what cost?
27. Is there anything that your organisation will need to stop doing as a result of the LED? Will this cause you to incur costs/benefits? If so, what and what is the estimated cost?

LED Benefits

28. Will the LED provisions save your organisation time and money? Can you estimate this?
29. Will the LED provisions increase efficiency in the fight against crime and public security? Can you estimate this?
30. Will the LED provisions help to create the smoother transfer of data? If so, can you estimate this?
31. Do you think this will help your organisation lead to faster/better/stronger prosecutions? If so, can you estimate this?
32. Would it be easier to prevent, investigate, detect, prosecute crimes or safeguard public security given the LED? If so, can you estimate this?
33. Do you think this will help lead to better protections to victims, witnesses and/or other members of the public? If so, can you estimate this?
34. Do you think that by applying the LED there will be fewer data breaches within your organisation and as such an improvement to its reputation? If so, can you estimate this improved reputation?

Supplemental questions on familiarisation costs

35. Currently is there a requirement for your staff to undertake regularly (i.e. annually) an e-learning package or to read guidance in relation to their responsibilities around data handling?
36. Do you have staff that would require to have specific training in regards to Law Enforcement Processing due to the changes in legislation, and if so how many? (such as Data Protection Officers or those dealing with Subject Access Requests)
37. Would this training be separate to training for the General Data Protection Regulations (GDPR)?
38. How many words is any training/guidance likely to be and what percentage would be Law Enforcement Processing specific?
39. Please provide any other costs that you are aware of in relation to familiarisation of the change in Law Enforcement Processing of personal data as a result of the LED?
40. How many employees do you have (paid and unpaid), and how many would require specific training by day one of the Act coming into effect?

Annex E

Costs of Compliance

Costs		Low	Mid	High
Cost of compliance (Q7)		50%	100%	150%
No cost	5	£0	£0	£0
Low cost (already planned)	9	£0	£0	£0
Monetised	1	£50,000	£100,000	£150,000
Don't know: Some cost	15	£50,000	£100,000	£150,000
Don't know: Don't know	6	-	-	-
Check Sum	0			
Total cost		**£800,000**	**£1,600,000**	**£2,400,000**
Average Cost		£26,700	£53,300	£80,000

Cost of Features(Q14)				
No cost	16	£0	£0	£0
Low cost (already planned)	2	£0	£0	£0
Monetised	1	£15,000	£30,000	£45,000
Don't know: Some cost	13	£15,000	£30,000	£45,000
Don't know: Don't know	4	-	-	-
Check Sum	0			
Total Cost		**£210,000**	**£420,000**	**£630,000**
Average Cost		£6,600	£13,100	£19,700

Annex F

SAR costs.

Lost SAR Income[22]				
SAR fee (Q17)	SAR volume (Q16)	Cheque Processing Fee (Q18)	Representative cheque fee	Income
n/k	n/k	n/k		
£0	0	£0.00	£0.00	£0
£0	69	£0.00	£0.00	£0
£0	1	£0.00	£0.00	£0
£0	5	£0.00	£0.00	£0
n/k	n/k	n/k		
£10	1000	n/k	£5.35	£4,700
n/k	n/k	n/k		
n/k	n/k	n/k		
£5	1500	n/k	£5.35	£500
n/k	n/k	n/k		
£0	1	£0.00	£0.00	£0
£10	2500	n/k	£5.35	£11,600
£10	8	n/k	£5.35	£0
£0	1	£0.00	£0.00	£0
£0	0	£0.00	£0.00	£0
£10	4044	n/k	£5.35	£18,800
£10	26	£0.05	£0.05	£300
£0	5	£0.00	£0.00	£0
£0	100	£0.00	£0.00	£0
£0	20	£0.00	£0.00	£0
£10	300	n/k	£5.35	£1,400
£0	0	£0.00	£0.00	£0
£0	35	£0.00	£0.00	£0
£0	3600	£0.00	£0.00	£0
£10	210	n/k	£5.35	£1,000
£10	188	n/k	£5.35	£900
£10	395	n/k	£5.35	£1,800
£10	250	n/k	£5.35	£1,200
£10	149	£8.00	£8.00	£300
£10	300	£8.00	£8.00	£600
£0	3900	£0.00	£0.00	£0
£0	n/k	£0.00	£0.00	£0
£0	0	£0.00	£0.00	£0
£0	n/k	£0.00	£0.00	£0
£0	87	£0.00	£0.00	£0
	18694			**£42,000**
	644.6	**£5.35**		**£1,400**
				£3,200

[22] n/k = not known, where orange or red they did not provide a quantified estimate, but indicated that there would be a medium or high cost.

Cost of processing SARs (Q19)	Cost per SAR	Anticipated processing cost of removing fee (Q21)	Representative cost - Low	Representative cost - Mid	Representative cost - High
n/k		n/k	n/k	n/k	n/k
n/k		0	0	0	0
n/k		0	0	0	0
n/k		0	0	0	0
£1,850	£370	0	0	0	0
n/k		n/k	n/k	n/k	n/k
£70,000	£70	n/k	£3,500	£7,000	£14,000
n/k		n/k	n/k	n/k	n/k
n/k		n/k	n/k	n/k	n/k
£50,000	£33	n/k	n/k	n/k	n/k
n/k		n/k	n/k	n/k	n/k
n/k		0	0	0	0
£584,000	£234	n/k	£29,200	£58,400	£116,800
n/k		n/k	n/k	n/k	n/k
n/k		0	0	0	0
n/k		0	0	0	0
n/k		n/k	n/k	n/k	n/k
£2,600	£100	£750	£750	£750	£750
£3,000	£600	0	0	0	0
n/k		n/k	£1,100	£2,300	£4,500
£7,000	£350	n/k	n/k	n/k	n/k
n/k		£140,000	£140,000	£140,000	£140,000
n/k		0	0	0	0
n/k		n/k	n/k	n/k	n/k
£37,500	£10	0	0	0	0
n/k		0	0	0	0
n/k		n/k	£0	£2,100	£4,200
£67,500	£171	n/k	£0	£3,400	£6,800
£50,000	£200	n/k	£0	£2,500	£5,000
£50,000	£336	n/k	£0	£2,500	£5,000
£44,700	£149	n/k	£0	£2,200	£4,500
£1,200,000	£308	n/k	£0	£60,000	£120,000
n/k		n/k	n/k	n/k	n/k
n/k		0	£0	£0	£0
n/k		0	£0	£0	£0
n/k		n/k	£0	£1,000	£2,000
£2,168,000		**£141,000**	**£174,600**	**£282,000**	**£423,000**
£166,800	**£225**	**£9,400**	**£7,000**	**£11,000**	**£17,000**
			£13,400	**£21,700**	**£32,600**

Annex G

Cost of DPIAs

Cost of producing DPIAs and communicating with ICO? (Q25)	Representative value -Low	Representative value -Mid	Representative value -High
Low/Medium	£6,250	£12,500	£25,000
High	£12,500	£25,000	£50,000
0	£0	£0	£0
0	£0	£0	£0
0	£0	£0	£0
Unknown			
High	£12,500	£25,000	£50,000
0	£0	£0	£0
Unknown			
0	£0	£0	£0
0	£0	£0	£0
0	£0	£0	£0
0	£0	£0	£0
Unknown			
Low/Medium	£6,250	£12,500	£25,000
High	£12,500	£25,000	£50,000
High	£12,500	£25,000	£50,000
Unknown			
0	£0	£0	£0
0	£0	£0	£0
Low/Medium	£6,250	£12,500	£25,000
Low/Medium	£6,250	£12,500	£25,000
0	£0	£0	£0
Unknown			
0	£0	£0	£0
Low/Medium	£6,250	£12,500	£25,000
0	£0	£0	£0
0	£0	£0	£0
Low/Medium	£6,250	£12,500	£25,000
Low/Medium	£6,250	£12,500	£25,000
Low/Medium	£6,250	£12,500	£25,000
Low/Medium	£6,250	£12,500	£25,000
Low/Medium	£6,250	£12,500	£25,000
Unknown			
0	£0	£0	£0
0	£0	£0	£0
Total	£112,500	£225,000	£450,000
Average	£3,750	£7,500	£15,000
Average of those affected	£8,000	£16,000	£32,000

Annex H

Summary of the sensitivity analysis

	Low		Best		High	
	Average	**Total (£ m)**	**Average**	**Total (£ m)**	**Average**	**Total (£m)**
Annual costs						
Lost SAR revenue	-£1,400	-£0.5	-£1,400	-£0.6	-£1,400	-£0.7
Increased SAR volumes	-£7,000	-£2.8	-£11,000	-£5.1	-£16,000	-£8.5
Cost of producing DPIAs	-£4,000	-£1.5	-£7,500	-£3.4	-£15,000	-£7.5
Costs to ICO	-	-£0.5	-	-£0.6	-	-£0.6
One-off costs						
Compliance costs	-£27,000	-£10.7	-£53,000	-£24.0	-£80,000	-£40.0
Costs of Features	-£7,000	-£2.6	-£13,000	-£5.9	-£19,700	-£9.8
Annual Benefits						
Fewer breaches	-	£0.0	-	£0.0	-	£0.0
SAR revenue to applicants	£3,000	£1.3	£3,000	£1.5	£3,000	£1.6

	Low	**Best**	**High**
NPV (£m)	**-£46.4**	**-£96.0**	**-£177.3**
BNPV (£m)	**-£4.5**	**-£19.3**	**-£49.8**
EANDCB (£m)	**-£0.5**	**-£2.3**	**-£5.8**