Data Protection and Digital Information Bill

Information Sheet

Background

1. The Data Protection and Digital Information Bill marks an evolution of the UK's data protection framework by updating the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the Privacy and Electronics Communications Regulations (PEC Regulations). The Bill will maintain high data protection standards, whilst also encouraging innovation and reducing compliance burdens for businesses. It also lays the foundation for the dynamic and innovative use of data to improve service efficiency and quality for the public. The combined economic effect of this bill is a boost to the economy of approximately £10.6 billion over 10 years.

2. This Bill is the product of in-depth consultation with stakeholders including businesses, civil society organisations and members of the public. It has been carefully designed to provide a future-proofed and flexible data protection framework for the UK.

3. The Government is issuing this information sheet to clarify the scope and impact of the Bill, with the aim of giving members of the House the necessary context to aid them in scrutinising the Bill ahead of Committee stage. This sheet will focus on Parts 1 and 4 of the Bill, which cover the changes to the data protection framework, including the regime governing processing by law enforcement agencies.

Maintaining High Data Protection Standards

4. While the DPDI Bill updates the data protection framework, it continues to uphold the fundamental data protection principles that are set out in the UK GDPR and DPA 2018. The independent Information Commissioner has lent his support for the Bill and its approach, affirming that it will "*maintain our high standards of protection in the UK*" and that it "*protects people's rights and freedoms".*

5. Any organisation which processes personal data must continue to comply with the data protection principles. The Bill gives data controllers more flexibility about how they choose to manage data protection risks, but they will still have to do so and will continue to be accountable for how they process data and must have appropriate measures in place to demonstrate compliance. Individuals whose rights may have been breached will continue to have the right to complain to the ICO and to seek compensation through the courts. The DPDI bill also ensures, for the first time, that data controllers must put in place a transparent process for responding to complaints.

6. The ICO is also being given new powers to aid its investigations, helping it to tackle new and emerging risks and protect people to the standard that they expect. These

include the power to order an independent company to produce a report to inform investigations and the power to issue a written interview notice, which would compel witnesses to attend interviews and answer questions in relation to an investigation. This will help speed up investigations, whilst also allowing the ICO access to as much information as necessary so that it can make a decision. It will also be able to impose higher fines for breaches of PEC Regulations, such as generating large volumes of nuisance calls.

7. During the consultation on the DPDI Bill, the Government repeatedly heard from stakeholders that the complex and ambiguous language in the UK GDPR caused confusion for data controllers, resulting in lower protections for data subjects in practice. The DPDI Bill mitigates this by including clarificatory provisions in several areas, such as the rules on when data collected for one purpose can be re-used for another, to give controllers and individuals more confidence in how the law should be applied.

8. A number of controllers indicated during the consultation that responding to Subject Access Requests (SARs) posed a disproportionate burden on their time and resources. The current threshold for rejecting data subject requests or charging a reasonable fee to comply with the request, is if the request is 'manifestly unfounded or excessive'. Many respondents felt they could rarely rely on this threshold in cases where it may have been appropriate for them to do so.

9. Our reforms in this area will reduce the resources controllers currently invest in responding to these types of requests, by changing the circumstances in which controllers may refuse to comply with a request from a data subject or charge a reasonable fee for complying with it, from when the requests are 'manifestly unfounded or excessive' to when they are 'vexatious or excessive'. Alongside this, the Bill clarifies the circumstances which would meet this threshold, such as requests made with ill intention, or where the information being requested has been previously provided. This adopts similar language to that which is already used in the Freedom of Information Act 2000.

10. Whilst it is important to note that these reforms do not change the default position that controllers should respond to any request from a data subject, this reform ultimately aims to stop requests that are intended to cause distress, are an abuse of process or not made in good faith freeing up resources for organisations to respond to legitimate requests and other activities.

Reducing Burdens for Businesses

11. The UK's data protection legislation applies to all UK businesses that process personal data. The European Commission's own assessment of the EU GDPR in 2020 showed

that the average SME in the EU could expect its compliance costs to comprise nearly 40% of IT budgets. Academic research has indicated the complexity of GDPR could lead start-ups to abandon product ideas because they incorrectly identified their development process as incompatible with GDPR.

12. The DPDI Bill will reduce burdens for organisations which do not engage in high-risk processing, resulting in small and micro businesses being a projected £100m a year better off through a combination of savings and increasing Gross Value Added. This is why 66% of small and medium businesses support reforms to data protection laws, according to research by the Direct Marketing Association, a trade association comprising over 700 UK businesses.

13. Businesses will now only need to invest time and resources in specific compliance activities if they engage in high risk processing. For example, they will only have to keep records of their processing activities, undertake risk assessments and designate Senior Responsible Individuals (SRIs) if their processing activities are likely to pose high risks to the rights and freedoms of individuals or if they are a public body. Organisations that are unsure whether their processing activities are high risk will refer to the ICO's guidance on the subject, which the DPDI Bill requires the ICO to produce.

14. High risk processing refers to any kind of data processing activity which may pose a high risk to the rights and freedoms of individuals. This term is not defined in the legislation as our consultation showed that organisations were keen for the data protection framework to be 'more flexible and risk-based', giving them the ability to assess risk in the context of their business activities and circumstances. Organisations will naturally need to consider carefully any processing of sensitive data about children and other vulnerable groups.

15. In addition, businesses which currently rely on the 'legitimate interests' lawful ground to process personal data without consent will no longer have to undertake detailed 'legitimate interest balancing tests' in relation to a small number of processing activities that Parliament deems to be 'recognised legitimate interests'. This includes processing which is necessary for important objectives of public interest, such as crime prevention, safeguarding, and responding to emergencies.

16. The Government is also aware, from both our consultation and ongoing engagement, that many organisations have invested heavily in putting policies and procedures in place to comply with UK GDPR. The DPDI Bill will not force companies to replace these policies and procedures if they wish to retain them.

17. Organisations which have taken steps to comply with the UK GDPR will mostly be compliant with the legislation as amended, except for a small number of new requirements such as the requirement for a transparent complaints procedure, and designating a Senior Responsible Individual (SRI) to manage data protection risks –

although they will be allowed to delegate their functions to another qualified person, including independent privacy experts similar to DPOs and/or people currently working in that organisation as privacy professionals. This also means that companies which have establishments in the EU as well as the UK, or which offer goods or services to EU data subjects do not need to incur costs by creating a separate system to comply with UK data protection law.

18. This is why businesses have positively received these reforms. TechUK, a trade association comprising over 1000 UK businesses in the technology sector, has described the Bill as an "*important evolution of the UK's data protection framework...[which] is designed to make the UK's data protection regime clearer and easier to comply with for low-risk scenarios, to support data driven research and innovation and provide clarity to organisations on how they can process data for clear public interest reasons."*

Modernising and Strengthening the ICO

19. The Government has worked closely with the ICO while preparing the DPDI Bill. The ICO has lent its full support to these reforms to its governance and structure. The Information Commissioner, John Edwards, has "*welcomed [the Bill as] a positive package of reforms that would allow us to continue to operate as a trusted, fair and independent regulator."* The ICO will be publishing extensive guidance after the Bill becomes law to aid data controllers, particularly smaller organisations without dedicated in-house privacy professionals, in preparing for the reforms.

20. The DPDI Bill has introduced several reforms to the governance and functions of the ICO, with the view of modernising the regulator and ensuring that it has sufficient powers to tackle breaches of data protection law. These reforms maintain the independence of the ICO and continue to hold it accountable to Parliament, rather than the Government. They will allow the ICO to work strategically, allocate resources efficiently and allow it to take decisive action to uphold the UK's data protection standards.

21. A significant change is that the ICO will become the Information Commission (IC), with a new statutory board with a chair and chief executive. This will bring it in line with other regulatory bodies in the UK such as OFGEM and OFCOM. This ensures that powers are dispersed across a board of people, rather than vesting in a single Commissioner, and reflects best practice for regulators.

22. The new Information Commission will remain accountable to Parliament through a requirement to report on its regulatory approach and performance. It will prepare this report against a new regulatory framework which sets out a 'principal objective' of securing an appropriate level of data protection while accounting for the interests of data subjects, organisations and the wider public interest. Similarly, it must consider

factors such as competition, innovation, economic growth and good regulation while discharging its duties.

23. To aid the IC in deciding how to prioritise its resources, a new statutory framework of objectives and duties has been introduced. The Government may also prepare a Statement of Strategic Priorities to which the IC must prepare a response setting out how it will have regard to the statement, although it is not required to take the statement into account on individual enforcement actions. This will protect the operational independence of the IC while giving it additional valuable context to consider when deciding how to prioritise resources. The Information Commissioner himself has stated that the reform "*will not create any opportunity for any member of government to interfere or influence the activities of the ICO on a day-to-day basis*" and that our reforms will support the ICO in achieving its stated goal to *"help business to help people*".

Promoting Responsible Use of Solely Automated Decision Making

24. Existing data protection legislation (UK GDPR and the Data Protection Act 2018) regulates the development of AI systems and other technologies, to the extent that there is personal data involved. The main reference point for the requirements related to solely automated decision-making that has significant effects on individuals in the UK's data protection law is Article 22 of the UK GDPR law. Automated decision-making (ADM) of this nature is increasingly AI-driven and, with the expansion in use of this technology, it is important that our rules are fit for purpose.

25. However, in the Government's consultation prior to the DPDI Bill, it was evidenced stakeholders find the current data protection rules are ambiguous and complex – meaning the safeguards for individuals subject to this processing are rarely used effectively.

26. We are therefore using the DPDI Bill to reform Article 22, to reduce the barriers to responsible data use, and ensure important safeguards are implemented when they matter most.

27. The rules in Article 22 are currently framed as a general prohibition on solely ADM of this nature, except where certain limited conditions apply. We are expanding the lawful grounds available under the data protection regime when carrying out solely ADM that has significant effects on individuals, reflecting the growth in use of this processing by emerging technology in everyday life.

28. However, in doing so we are ensuring data subjects always have a right to specific safeguards regardless of the lawful basis on which such activity is carried out. These safeguards include providing information on the ADM that has been carried out, the right to contest those decisions and to seek human review of them, requiring controllers

to correct decisions that have produced wrongful outcomes. Furthermore, the existing transparency and rights of access provisions in the wider data protection framework, which require organisations to inform individuals about the existence of solely ADM, continue to apply.

29. Alongside these safeguards, our reforms will also make clear that decisions are regarded as "solely" automated when they are produced without any meaningful human involvement. We are clarifying that meaningful involvement means that the involvement of a human goes beyond cursory or 'tick box' involvement and assumes an understanding of the process. This will ensure clarity for when such decisions are to be considered solely ADM, and that individuals will have the relevant safeguards applied to them in these circumstances.

30. We are also maintaining the restrictions of the current regime on solely ADM that have significant effects using special category data such as information on a person's health, sexual orientation or racial identity, which requires enhanced protections. This type of ADM can only be carried out where an individual has given their explicit consent, engaged in a contract with the controller or is required or authorised by law. Additionally, the processing must satisfy the substantial public interest condition in Article 9 UK GDPR.

31. The Government is confident that these changes strike the right balance between enabling the best use of ADM technology, while continuing to protect the rights of data subjects.

Democratic Engagement

32. The responsible use of personal data by registered political parties, elected representatives, candidates and permitted participants in referendums is an essential part of a healthy democracy.

33. The Data Protection Act 2018, which implements the EU GDPR, recognises democratic engagement as one of the grounds on which personal data can be processed for a task in the public interest. However, the relevant provisions are reliant on there being separate domestic legislation setting out the purposes of the processing. In terms of democratic engagement activities, this makes them unsuitable for the UK, where the democratic role and status of elected representatives and candidates is governed by convention rather than statute. Since these individuals do not have explicit legal status, they cannot confidently process data for democratic engagement purposes~~,~~ other than personal data obtained from the electoral roll.

34. Seizing the post-Brexit opportunity to reform the data protection framework, the Government has introduced a non-partisan reform that will equally apply to all political parties, candidates and elected representatives. The Bill will provide a clear lawful

ground under Article 6 of the UK GDPR for processing which is necessary for the purposes of democratic engagement and other 'recognised legitimate interests' which serve important public interest objectives. Controllers which are processing personal data for any of the activities on the list will not need to seek consent or carry out a detailed 'legitimate interests assessment' prior to processing.

35. Significantly, this reform does not exempt data controllers from making sure the processing is necessary and proportionate for the stated objective and complying with other data protection principles, for example on fairness, transparency, purpose limitation and storage limitation.

36. These reforms bring clarity to the existing data protection legislation, by specifying the scope of activities that are considered democratic engagement and which individuals and organisations surrounding can process personal data for these purposes, giving data controllers confidence when interpreting the law. This will allow the relevant organisations and individuals to directly contact voters to share their political platforms and hear their constituent's opinions, further improving the quality of democratic engagement in the UK.

37. The other main reform is to the Privacy and Electronic Communications Regulations (PEC Regulations), which regulates direct marketing using electronic means, such as e-mail, text message or phone call.

38. Currently, commercial organisations can send electronic direct marketing communications (e.g. emails and text messages, but not calls) to customers who they have been in contact with during the course of a sale, or negotiation for the sale, of a product or service. This is known as the soft opt-in.

39. The Bill will apply the same rule to non-commercial organisations such as political parties to improve engagement with the electorate. For example, if an individual has attended a political party's event and has provided their contact details, they can be contacted by the party with political messaging. The safeguards that currently apply to the commercial soft opt-in will be replicated, so that a person can opt out of receiving communications at the time their data is collected or when they receive any subsequent communication.

40. The Bill also includes a regulation-making power so that future governments can keep the PEC Regulations under review and make further exceptions through secondary legislation for electronic communications, such as telephone calls, emails and text messages, sent for democratic engagement purposes. This does not mandate any changes, which will only take place if the evidence supports it and following consultation with the Information Commissioner and other interested parties. This power reflects the status quo under the European Communities Act of 1972 and

previous EU Directives, which gave Member States the discretion to pass similar regulations.

Improving Operational Effectiveness of Law Enforcement

41. The DPDI Bill aims to improve data use and data sharing for law enforcement and national security by creating greater consistency across the data protection regimes and making data protection law clearer for users. It will encourage better use of personal data where appropriate to help protect the public.

42. In response to concerns raised by policing bodies, the Bill removes the requirement for law enforcement agencies to record a justification every time data is consulted or disclosed. Importantly, it does not remove the need for police to justify their processing, it is simply removing the ineffective, administrative requirement to record the reason in a log as, whilst it was intended to monitor and detect unlawful access, this has not proved to be the case in investigations.

43. It is estimated this change could save police forces approximately 1.5 million hours and £46.5 million annually. The other logging requirements, such as time, date, and identity of the individual, will be kept, and will continue to ensure accountability for data-use by law enforcement.

44. In response to recommendations from the inquests into the Manchester and Fishmonger Hall terrorist attacks, the DPDI Bill also includes a provision allowing law enforcement agencies to jointly process data alongside the intelligence agencies for the purposes of safeguarding national security. The Impact Assessment for the Bill indicates that this proposal may result in "*more effective CT [Counter Terrorist] investigations thus...reducing crime and risk of terrorism to the UK and UK interests overseas.*" This is because the regime for intelligence services has stronger protections for national security, which will mitigate any potential risk of law enforcement disclosing sensitive information which may expose operational risks and undermine intelligence services work.

Simplifying oversight of biometrics and surveillance cameras

45. The Biometrics Commissioner oversees police use of biometrics (DNA and fingerprints) that they take on arrest, and reviews police requests to retain the biometrics of people not convicted of an offence on national security and public safety grounds. The Surveillance Camera Commissioner promotes good practice by local authorities and the police when using surveillance cameras.

46. The ICO already regulates all organisations' use of biometrics and surveillance cameras, and has produced guidance on these issues. The overlap in functions has resulted in confusion for the police and the public and inhibits innovation. Responses

to the initial consultation on the DPDI Bill recognised this and supported simplifying the oversight framework in this way.

47. To achieve this the Bill transfers the Biometric Commissioner's casework functions to the Investigatory Powers Commissioner's Office, which is experienced in carrying out similar work, and abolishes the Surveillance Camera Commissioner's functions altogether in light of the duplication identified in the consultation. This will streamline and simplify this oversight framework, giving the police clear and consistent guidance while ensuring these activities continue to be regulated.i

48. The ICO will continue to regulate all organisations' use of biometrics and surveillance camera data, and a number of other bodies will also continue to operate in this space, including the Forensic Information Database Service Strategy Board, the Forensic Science regulator, the College of Police, His Majesty's Inspectorate of Constabulary and Fire and Rescue Services, and the Equality and Human Rights Commission.

Tackling Benefit Fraud and Error

49. Fraud is a growing problem across the economy, accounting for over 40% of all crime and the welfare system is not immune to this. With the advent of new technologies, fraud has increased both in sophistication and scale. Although down by 10% from 2021/22; in 2022-2023 alone, the Government overpaid a total of £8.3billion due to welfare fraud and error, and over £8bn a year has been overpaid since the pandemic. It is vital that the Government takes measures to reduce this to ensure the right level of support reaches the right people.

50. This measure is a vital step in the delivery of DWPs fraud plan, *"Fighting Fraud in the Welfare System"* that was published in May 2022. This plan clearly sets out the new powers DWP plan to legislate for to tackle the fraud and error found in the welfare system, including committing to give DWP the power to require third parties to provide data which can help the DWP to identify cases where people may not meet the eligibility for the payments they are receiving.

51. The Government has included a measure in the DPDI Bill which puts this proposal into effect and will result in savings of up to £600m over the first five years, an estimate which has been independently scrutinised by the Office for Budget Responsibility.

52. This power is necessary. The current powers DWP have to ensure benefit correctness are mostly over twenty years old. Under current legislation, the DWP does not have the power to independently verify information such as the amount of savings or time spent outside the country and has had to rely on self-verification instead. We need to modernise and strengthen DWPs legislative framework to give those tackling fraud the tools they need to stand up to future challenges and minimise the impact of genuine mistakes that can lead to debt.

53. The measure will allow DWP to require third parties to look within their own data and cross reference this with a set of criteria DWP will provide. These criteria will link to the eligibility for a particular payment and third parties will need to be able to independently identify claimants in their own data, match those accounts to the set criteria and pass on only minimal data, such as names and which criteria has been met, onto DWP. This approach avoids the DWP sharing any personal data with third parties to obtain the information it needs. As this data may signal potential fraud or error, DWP will then review these cases – through business-as-usual processes - to determine whether incorrect payments are being made.

54. The vast majority of claimants who comply with the rules of entitlement for the benefits they receive will be unaffected by this measure. DWP will only request information where there is a link between DWP, the data holder and the recipient of payment and a signal of a potential overpayment. Where this is not the case, no claimant information will be shared. Furthermore, for those who have been overpaid through genuine error, this measure will mean that this overpayment is identified and stopped earlier, preventing claimants from building up debts.

55. It is important to note that this power **does not** allow DWP to access millions of bank accounts nor does it allow DWP to see how claimants are spending their money. The measure will also not create a power to surveil or request unnecessary information about benefits claimants or state pensioners.

56. The power covers all benefits, grants and other DWP payments. This is to ensure that, where fraud and error arises, the Department has the power to address it. However, in the first instance, the DWP is clear that it will use this power to tackle overpayments and fraud and error in those payments where there are the greatest areas of loss. In the first instance, this will be means-tested benefits. We do know, however, that no payment that we make is immune to fraud and error therefore it is right that the power covers all social security benefits and payments. This will enable Government to tackle rising fraud and error where it occurs in the future.

57. DWP will protect the data it receives. DWP continuously handles large volumes of data and has robust processes in place. The delivery of this measure will be undertaken in collaboration with third parties, including the banking industry, so it is as secure as possible. We have already established a working group with industry to oversee this work.

Maintaining EU Data Adequacy

58. The adequacy arrangements with the EU allow organisations to transfer personal data between the UK and the EU in an easy and safe way, without having to use alternative

transfer mechanisms.

59. The UK is not required to have the same rules as the EU to be considered adequate. The European Commission has been consistent in its stance that identical data protection rules are not a requirement for adequacy. Indeed, there are fifteen countries which have EU adequacy, including Japan, New Zealand, and Canada. All these nations pursue independent approaches to data protection.

60. The reforms in the Data Protection and Digital Information Bill are complemented by robust safeguards, and we believe they are compatible with maintaining our EU data adequacy decisions. While the Data Protection and Digital Information Bill will remove the more prescriptive elements of the EU GDPR, the UK will maintain its high standards of data protection and continue to have one of the closest regimes to the EU in the world.

61. This view is also supported by the Information Commissioner in his independent assessment of the Bill, where he stated that *"Adequacy does not require a carbon copy of the GDPR and these changes maintain the high standards that both the UK and EU are committed to...In my view the proposed changes in the bill strike a positive balance and should not present a risk to the UK's adequacy status."*

62. Trade associations like TechUK have also independently assessed the Bill and see it as being compatible with maintaining EU adequacy because "*the reforms enacted in the DPDI Bill in our view do not substantially change data protection rights in the UK and British data protection standards should remain essentially equivalent to the EU's.*" TechUK strongly advocated for maintaining data adequacy during the UK-EU Brexit negotiations and says that its assessment is built on a number of years' experience working on data protection frameworks and engaging with EU stakeholders.

63. The Government has a positive relationship with the European Commission and has consistently engaged with it throughout the passage of the Bill, leading technical briefings on its provisions. We will continue to engage with the EU to ensure our reforms are understood.