BIG BROTHER WATCH

Big Brother Watch Briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons Report Stage

November 2023

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Direct line: 020 8075 8478

Email: silkie.carlo@bigbrotherwatch.org.uk

Susannah Copson

Legal and Policy Officer

Direct line: 07935926492

Email: susannah.copson@bigbrotherwatch.org.uk

Table of Contents

RECOMMENDATIONS

- **Support NC43** tabled by David Davis MP to create a legal right to non-digital ID;

- **Support amendment 280/NS3** tabled by Marcus Fysh MP to ensure that the Secretary of State and DVS trust framework uphold user-centred privacy principles;

- **Support amendments 278 and 279** tabled by Marcus Fysh MP to prevent personal data from being processed outside of the usual legally-defined routes and with lower levels of protection;

- **Vote against Government amendment NC34 and NS1** that would force banks to monitor all bank accounts to track welfare recipients for potential fraud;

- **Vote against Government amendments NC36, NC37 and NC38** that would allow law enforcement agencies to retain pseudonymised (and therefore identifiable) biometric data indefinitely.

SUMMARY

1. Big Brother Watch believes that the Data Protection and Digital Information (No. 2) Bill (DPDI2 Bill) threatens to greatly weaken the existing data protection framework and is not fit for purpose.

2. The DPDI2 Bill was published on 8th March 2023 by the newly created Department for Science, Innovation and Technology (DSIT) as part of government efforts to establish a UK independent data protection framework. In anticipation of Report Stage in the House of Commons, commencing on Wednesday 29th November 2023, we would like to draw your attention to a number of concerning issues both within the Bill and the government's proposed amendments. We propose amendments that are required in order to protect well-established privacy and data rights, maintain adequacy with EU law, and uphold the rule of law. We would also like to draw your attention to problems with some of the government's amendments and discourage MPs from supporting them.

We have proposed the following amendments, which have been tabled at Report stage, and we urge Members of Parliament to support:

- **New Clause 43: To establish a digital identity verification framework to protect user rights and uphold important data protection, privacy, and equality rights.** This should include establishing a right to use non-digital ID in order to protect the public's ability to choose how they express their digital identity.

- **Amendment 280/NS3:** The Bill introduces a new regime for digital verification services, and requires the Secretary of State to prepare a Digital Verification Services (DVS) Framework. The framework currently lacks important safeguards and human rights principles, including consideration of the Identity Assurance Principles developed by the Privacy and Consumer Advisory Group (PCAG). **The Secretary of State and DVS framework must uphold the Identity Assurance Principles** in order to safeguard against the potential of a digital identity environment that would give rise to invasive, exclusionary and discriminatory impacts.

- **Amendments 278 and 279: Remove the new concept of 'recognised legitimate interests' to prevent the Secretary of State from having the ability to pre-authorise data processing outside of the usual legally-defined route.** These amendments would retain the current test in which personal data can only be processed in pursuit of a legitimate interest, as balanced with individual rights and freedoms. This is important to avoid a two-tier data protection framework in which the Secretary of State can decide that certain processing is effectively above the law.

Additionally, we would like to highlight the harmful potential of two of the Government's proposed amendments that propose to:

- **NC34 and NS1:** Create new powers to force banks to monitor all bank accounts to find welfare recipients and people linked to those payments, potentially including landlords, and report anyone who triggers potential fraud indicators (such as frequent travel or savings over a certain amount) to the Department for Work and Pensions.

- **NC36, NC37 and NC38:** Enable law enforcement agencies to retain pseudonymised biometric data indefinitely.

AMENDMENTS

(i) RIGHT TO NON DIGITAL ID

New Clause 43 tabled by David Davis, John McDonnell, Alistair Carmichael, and Marcus Fysh.[1]

To move the following Clause—

Right to use non-digital verification services

(1) This section applies when an organisation—

(a) requires an individual to use a verification service, and

(b) uses a digital verification service for that purpose.

(2) The organisation—

(a) must make a non-digital alternative method of verification available to any individual required to use a verification service, and

(b) must provide information about digital and non-digital methods of verification to those individuals before verification is required.

Effect of the amendment

This new clause, which is intended for insertion into Part 2 of the Bill (digital verification services), creates the right for data subjects to use non-digital identity verification services as an alternative to digital verification services, thereby preventing digital verification from becoming mandatory in certain settings. It is designed to ensure that when it comes to essential services, banking, state services etc, the general public always have a choice when it comes to verifying their identity and are never compelled to have their personal information processed into databases or digital identity systems if they do not want to.

1 Data Protection and Digital Information (No. 2) Bill (Amendment Paper) (28 November 2023): https://publications.parliament.uk/pa/bills/cbill/58-03/0314/amend/datapro_rm_rep_1128.pdf 57.

Briefing

1. Part 2 of the Bill introduces a new regime for digital verification services. It sets out a series of rules governing the future use and oversight of digital identities as part of the government's roadmap towards digital identity verification.

2. NC43 would introduce a right to use non-digital verification services. This new clause will prevent digital ID from becoming mandatory in certain settings.

3. Having different ways to prove identity online can be useful. However, although the ability to verify identity online can be helpful for some people, it is equally a difficulty for those who cannot – or do not want – to use digital methods.

4. While there is no immediate plan for the introduction of a UK-wide mandatory digital ID, this amendment is being brought forward at a time when the Government is both creating a digital identity system to allow access to state services in the form of One Login and cultivating a new digital identity market in the private sector through the DVS Trust Framework.

5. Digital identity systems pose serious risks to rights, security, and equality. In the worst case scenario, they can be misused for mass surveillance, to track marginalised groups, to construct population-wide databases of personal data, exacerbate inequalities for people who cannot participate digitally, or can be vulnerable to hackers.

6. It is imperative that services are never contingent on a digital identity check, as this could prevent people from participating in key activities. There should always be an offline alternative for those electing to use the online services of an organisation for which there is an offline alternative do not wish to share their information digitally, so that participation is not coercive.

7. NC43 would give individuals a choice in how they choose to prove their identity and share personal data. Creating the legal right to choose enshrines the ability to opt out and use offline methods of identification

verification where needed and, in doing so, mitigates the risk of funnelling people into handing over data online, or leaving people out from accessing services.

8. The growing presence of digital identity systems and services should not mean that offline government services that require identity verification are made any less accessible, affordable or usable for people who cannot or do not want to use them. This new clause would ensure that the integrity of offline methods of proving identities are upheld.

(ii) EMBEDDING USER-PRIVACY INTO THE DVS TRUST FRAMEWORK

Amendment No.280 tabled by Marcus Fysh, Adam Holloway, Jonathan Lord, Priti Patel, Chris Green, Sir Edward Leigh, Greg Smith, and Robbie Moore.[2]

Clause 49, page 77, line 13, at end insert—

"(2A) The DVS trust framework must include a description of how the provision of digital verification services is expected to uphold the Identity Assurance Principles.

(2B) Schedule (Identity Assurance Principles) describes each Identity Assurance Principle and its effect."

Effect of the amendment

Clause 47(1)-(3) requires the Secretary of State to prepare a DVS Trust Framework. This amendment makes sure the Framework includes reference to the Privacy and Consumer Advisory Group's (PCAG) Identity Assurance Principles, which focus on the role of an individual's control and consent in providing identifying information to an Identity Assurance Service. The Bill gives the Secretary of State a series of new Henry VIII powers throughout its text, allowing much of the regulatory framework to be changed subject to the Secretary of State's discretion. It is therefore vital that the Secretary of State is obligated to uphold user-centred concerns in the development of a DVS trust framework, as articulated in the 9 Identity Assurance Principles, to ensure that such services protect the people who use them. This will help to install

2 Data Protection and Digital Information (No. 2) Bill (Amendment Paper) (28 November 2023): https://publications.parliament.uk/pa/bills/cbill/58-03/0314/amend/datapro_rm_rep_1128.pdf 59-60.

limitations around the purposes and substance of data sharing, which is vital in any discussion around the development of a digital verification trust framework.

Briefing

9. Part 2 of the Bill introduces a new regime for digital verification services. It sets out a series of rules governing the future use and oversight of digital identities as part of the government's roadmap towards digital identity verification. Clause 47 (1)-(3) require the Secretary of State publish a digital verification services (DVS) trust framework. This framework would allow authorities to disclose personal information to "trusted" digital verification services for the purpose of identity verification.

10. Part 2 of the Bill introduces a new regime for digital verification services. It sets out a series of rules governing the future use and oversight of digital identities as part of the government's roadmap towards digital identity verification. Clause 47 (1)-(3) require the Secretary of State publish a digital verification services (DVS) trust framework. This framework would allow authorities to disclose personal information to "trusted" digital verification services for the purpose of identity verification.

11. The Government's digital identity and verification plans, including the DVS provisions in this Bill, have the potential to give rise to excessive data sharing, privacy intrusion, and a digital identity environment that could be invasive, exclusionary and have discriminatory impacts. It is important that the Government gets the DVS framework right. Digital verification services must be designed around users needs and reflect important data protection principles and human rights. The framework must be trusted by the public in order for it to work, which is why it is important to build it upon established principles.

12. The Identity Assurance Principles were developed by the independent Privacy and Consumer Advisory Group, which "advises the government on how to provide a simple, trust and secure means of accessing public services".[3] They build upon these concerns through a series of identity

3 Privacy and Consumer Advisory Group – UK Government: https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group

principles, offering a framework designed to cultivate trust in the Identity Assurance Service by giving "real meaning to 'individual privacy' and 'individual control'".[4]

(iii) PERSONAL DATA PROCESSING - RECOGNISED LEGITIMATE INTERESTS

Amendments 278 and 279 tabled by Marcus Fysh, Adam Holloway, Jonathan Lord, Priti Patel, Chris Green, Sir Edward Leigh, Greg Smith, Robbie Moore, and David Davis.[5]

Clause 5, page 6, line 15, leave out paragraphs (b) and (c)

and

Clause 5, page 6, line 23, leave out subsections (4), (5) and (6)

Effect of the amendments

These amendments would remove the power for the Secretary of State to create pre-defined and pre-authorised "recognised legitimate interests", for data processing outside of the usual legally-defined route. Instead, the current test would continue to apply in which personal data can only be processed in pursuit of a legitimate interest, as balanced with individual rights and freedoms. This is important to avoid a two-tier data protection framework in which the Secretary of State can create loopholes through which certain data processing would effectively be above the law.

Briefing

13. Processing personal data is currently only legal if it is performed for at least one lawful purpose, one of which is that the processing is for legitimate interests pursued by the controller or by a third party except where those interests are overridden by the interests or fundamental rights of the data subject. As such, if a data controller relies on their 'legitimate interests' as a legal basis for processing data, they must conduct a balancing test of their interests and those of the data

4 Identity Assurance Principles, 2015: https://www.gov.uk/government/publications/govuk-verifyidentity-assurance-principles/identity-assurance-principles
5 Data Protection and Digital Information (No. 2) Bill (Amendment Paper) (28 November 2023): https://publications.parliament.uk/pa/bills/cbill/58-03/0314/amend/datapro_rm_rep_1128.pdf 75.

subjects. This is the most flexible lawful basis for data processing and affords protection to people and their personal data.[6]

14. Clause 5 of the DPDI2 Bill amends the UK GDPR's 'legitimate interest' provisions by introducing the concept of "recognised legitimate interests" (RLI), which allows data to be processed without a legitimate interests balancing test. Further, under new Article 6(1)(ea), the Secretary of State is empowered to determine RLIs, but must only "have regard to, among other things, the interests and fundamental rights and freedoms of data subjects" (emphases added). The current 'legitimate interests' test is much stronger, which cannot lawfully apply if the data subjects' interests override those of the data controller.

15. Through this clause, the Secretary of State would be able to determine new RLIs through secondary legislation, which is subject to minimal levels of parliamentary scrutiny. In reality, this means new reasons could be added to the list at any time and for whatever reason and would facilitate the flow and use of personal data for limitless purposes – a power also subject to political influence. This Henry VIII power invests undue power over personal data rights in the executive. It is unjustified and undermines the very purpose of data protection legislation, which is to protect the privacy of individuals in a democratic data environment.

16. Annex 1 of the Bill provides a list of RLIs including national security, public security and defence, emergences, and crime. These are overly broad and vague. For example, measures taken under the 'crime' interest could be incredibly damaging to privacy. For example, a company using facial recognition CCTV to film customers could rely on this RLI for their processing. Alternatively, an individual could use 'crime' as an a RLI to film neighbouring houses, despite the impact on privacy.

17. Clause 5 also provides examples of processing that "may be" considered legitimate interests under the existing legitimate interest purpose. These include direct marketing, an addition that appears to be a significant watering down of current standards, undoing the significant benefit the public has enjoyed with regards to reducing unwanted junk mail and calls since the introduction of GDPR. Direct

6 Information Commissioner's Office, Lawful basis for processing: Legitimate interests: https://ico.org.uk/fororganisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-forprocessing/legitimate-interests/

marketing is not just a nuisance – it can be mentally damaging. Targeted advertising can take an emotional toll on, for example, people who have suffered a miscarriage and continue to be pursued by adverts for baby products.[7]

GOVERNMENT AMENDMENTS

(i) NEW CLAUSE 34 AND NEW SCHEDULE 1 – POWER TO REQUIRE INFORMATION FOR SOCIAL SECURITY PURPOSES[8]

Effect of the amendment

This new Schedule amends social security legislation to give the Secretary of State a new power to direct banks to monitor bank accounts to surveil welfare recipients and people linked to those payments, potentially including landlords, and report anyone who triggers potential fraud indicators (e.g. frequent travel or savings over a certain amount) to the Department for Work and Pensions. Government amendment 207 means that this will come into force only two months after the Bill's royal assent.

Briefing

18. Everyone wants fraudulent uses of public money to be dealt with and the government already has powers to review the bank statements of welfare fraud suspects. Under current rules, the Department for Work and Pensions (DWP) is able to request bank account holders' bank transaction details on a case-by-case basis if there is reasonable grounds to suspect fraud. There are already multiple powers for this purpose: HMRC shares banking data with the DWP on an annual basis; the Proceeds of Crime Act 2002 requires banks and building societies to notify law enforcement of suspicious activity; Open banking enables consumers to give third parties access to their financial accounts; private companies that administer the UK's banking infrastructure can see transactional data; and Credit Reference Agencies can view credit histories.[9] However, this new power would allow the DWP to access the

7 Evidence on the Data Protection and Digital Information (No. 2) Bill and proposed amendments to the House of Commons Public Bill Committee (16 May 2023): https://publications.parliament.uk/pa/cm5803/cmpublic/Data ProtectionDigitalInformation/memo/DPDIB24.html

8 Data Protection and Digital Information (No. 2) Bill (Amendment Paper) (28 November 2023) NC34: https://publications.parliament.uk/pa/bills/cbill/58-03/0314/amend/datapro_rm_rep_1128.pdf

9 Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/

personal data of welfare recipients by requiring the third party served with a notice – such as a bank or building society - to conduct mass monitoring without suspicion of fraudulent activity. Section 3(a) states that this includes anyone "linked" to the receipt of a benefit - which could include ex-partners, co-habitants, children, or even landlords. Although Section 2(6) seems to imply that 'linked' means the same person only, this is badly worded and unclear which not only is bad lawmaking, but dangerous in such a high-risk context.

19. Once issued, an account information notice requires the receiver to give the Secretary of State the names of the holders of accounts (cl.2(1)(b)). In order to do this, the bank will have to process the data of all bank account holders and run automated surveillance scanning for benefits recipients. Further, the impact assessment states that an account information notice requires "other specified information relating to the holders of those accounts" and other connected information "as may be specified".[10] This vague definition would allow for an incredibly broad scope of information to be requested – something the DWP itself has acknowledged itself - and stands in contrast to the DWP's claim that they will adhere to the GDPR principle of data minimisation.[11]

20. Big Brother Watch finds it wholly inappropriate for the UK Government to order private banks, building societies and other financial services to conduct mass, algorithmic, suspicionless surveillance and reporting of their account holders on behalf of the state in pursuit of its policy aims. The government should not intrude on the privacy of anyone's bank account in this country without very good reason, whether a person is receiving benefits or not. People who are disabled, sick, carers, looking for work, or indeed linked to any of those people should not be treated like criminals by default. Such proposals do away with the long-standing democratic principle in Britain that state surveillance should follow suspicion rather than vice versa. It would be dangerous for everyone if the government reverses this presumption of innocence. This level of financial intrusion and monitoring affecting millions of people is highly

DWP_third_party_data_impact_assessment_november_2023.pdf 10.

10 Ibid

11 Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

likely to result in serious mistakes and sets an incredibly dangerous precedent.

21. The DWP's impact assessment notes that **"the power is not limited to a specific type of data"**. This lack of limitation would allow for extensive information about a person to be collected. An individual's outgoings can reveal highly sensitive information about them - what someone buys and where they spend is personal enough, but can reveal other intimate details by proxy; such as sexuality. This is incredibly intrusive, and extraordinarily so with no cap on the type of data that the DWP will be able to access.

22. The amendment allows for third parties who do not comply with account notice requests to be levied with financial penalties. The power is not limited to a specific institution – which means banks are not the only third party that can receive such a notice. Small businesses, such as a small online platform that facilitates peer-to-peer transactions that have minimal capacity to respond to such requests could be levied with heavy fines of a £1,000 fixed penalty and £40 daily penalties, which can rise to £1,000 daily rate after review.

23. This level of auditing and insight into people's private lives is a frightening level of government overreach – more so, for some of the most marginalised in society. It is disproportionate and expansive surveillance, and sets a worrying precedent for how the government oversee, access, and use people's personal data to make hugely impactful decisions about their lives. **Such a decision will allow disproportionate and intrusive surveillance of people in the welfare system** – that means that people including some of the poorest in our society, people with disabilities, or even carers will be subject to their spending essentially being pre-emptively examined, rather than on suspicion. It would put some of the most marginalised people on trial through intrusive bank surveillance. Questions must also be asked about how banks will use this data, and whether this will impact people's access to financial services.

24. In its impact statement, the DWP says that it will ensure data will be "transferred, received and stored safely".[12] Such a claim stands in stark contrast to the Department's track record of data security – particularly, considering that it was recently reprimanded by the ICO for data leaks so serious that they were reported to risk the lives of survivors of domestic abuse.[13] With no limitations set around the type of data the DWP can access, the impact could be even more severe.

25. Big Brother Watch has previously expressed serious concern over impact of automated decision-making, particularly in relation to how the Data Protection and Digital Information Bill will exacerbate such effects.[14] Regarding how people's data will be assessed, the DWP has stated that "we are clear [...] that no automatic decisions will be made based on data alone".[15] However, this statement has not been reflected in any form of legally binding decision. Big Brother Watch condemns the proposed amendment in its entirety but would like to highlight that, given the catalogue of risks raised by automated decision-making in key areas, it is completely inappropriate to make this kind of promise in non-binding methods that are subject to change, e.g. policy or Code of Practice. The lack of legal assurance is particularly concerning given the DWP history of conducting algorithmic surveillance on people in the welfare system.[16]

26. Given the severe impact of such expansive surveillance powers on fundamental rights and freedoms, it is entirely inappropriate for this amendment to be tabled at this stage of the Bill - less than a week before Report stage begins - as it has not allowed for either proper democratic scrutiny or parliamentary debate.

27. Being a part of the benefits system is a last resort – a necessity for survival. These new powers would mean that for people who are otherwise unable to support themselves, for whatever reason, they will

12 Ibid
13 Information Commissioner's Office, Letter to the DWP (31 October 2022): Https://ico.org.uk/media/action-weve-taken/reprimands/4023126/dwp-reprimand.pdf
14 Big Brother Watch, Big Brother Watch Briefing on the Data Protection and Digital Information (No. 2) Bill for House of Commons Committee Stage (May 2023): https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Big-Brother-Watch-Briefing-on-the-Data-Protection-and-Digital-Information-2.0-Bill-for-House-of-Commons-Committee-Stage.pdf
15 Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf
16 Big Brother Watch, 'Poverty Panopticon: The hidden algorithms shaping Britain's welfare state' (20 July 2021): https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf

have to depend on a system where they are subject to intrusive surveillance and broadly without their knowledge). **Scanning data without suspicion will effectively put welfare recipients – including the poor, parents and carers and disabled people - under constant financial surveillance.** Such measures would be a wholly unnecessary and disproportionate violation of the public's privacy and will be incredibly damaging for the most disadvantaged in our society.

We urge Members of Parliament to oppose this amendment to the Bill.

(ii) RETENTION OF BIOMETRIC DATA

28. The proposed NC36 – "Retention of biometric data and recordable offences", NC37 - "Retention of pseudonymised biometric data", and NC38 "Retention of biometric data from INTERPOL", would allow UK law enforcement agencies to hold biometric data received from overseas law enforcement agencies in a pseudonymised format. In cases where the authority ceases to hold the material pseudonymously, and the individual has no previous convictions or only one exempt conviction, the data may be retained in a non-pseudonymous format for up to 3 years. Therefore, the general rule is indefinite retention with continuous pseudonymisation, except for a specific circumstance where non-pseudonymised retention is permitted for a fixed period.

29. This is a major change in the way that personal data can be handled – permitting storage of pseudonymised or non-pseudonymised data will facilitate a vast biometric database that can be traced back to individuals. While this does not apply to data linked to offences committed in the UK, it sets a concerning precedent for reshaping how law enforcement agencies hold data, i.e. in a traceable and identifiable way. It seems that there is nothing to stop a law enforcement agency from pseudonymising data just to reattach the identifying information, which they would be permitted to hold for 3 years.

30. The amendments do not explicitly define the steps that must be taken to achieve pseudonymisation. This leaves a broad scope for interpretation and variation in practice. The only requirement is that the

data is pseudonymised "as soon as reasonably practicable", which is a totally subjective threshold.

31. The collective impact of these amendments is deeply concerning. Individuals with either no or minimal previous convictions could have their data stored pseudonymously (i.e. still traceable back to them) indefinitely, which completely contrasts the key privacy principles of necessity and proportionality. Instituting these kinds of intrusive measures is yet another example of expansive powers being ushered through under counterterror reasoning – and a slippery slope for how members of the public's data may be treated in the future, particularly with Chris Philp, Minister for Policing, calling to make the passport database more readily available to law enforcement agencies.[17]

We urge Members of Parliament to oppose new clauses NC36, NC37 and NC38.

17 The Guardian, 'UK Passport images database could be used to catch shoplifters' (2 October 2023): https://www.theguardian.com/uk-news/2023/oct/02/uk-passport-images-database-could-be-used-to-catch-shoplifters

ANNEX

Schedule 13A: the Identity Assurance Principles[18]

Part 1: Definitions

1. These Principles are limited to the processing of Identity Assurance Data (IdA Data) in an Identity Assurance Service (e.g. establishing and verifying identity of a Service User; conducting a transaction that uses a user identity; maintaining audit requirements in relation a transaction associated with the use of a service that needs identity verification etc.). They do not cover, for example, any data used to deliver a service, or to measure its quality.

2. In the context of the application of the Identity Assurance Principles to an Identity Assurance Service, "Identity Assurance Data" ("IdA Data") means any recorded information that is connected with a "Service User" including:

- "Audit Data". This includes any recorded information that is connected with any log or audit associated with an Identity Assurance Service.

- "General Data". This means any other recorded information which is not personal data, audit data or relationship data, but is still connected with a "Service User".

- "Personal Data". This takes its meaning from the Data Protection Act 2018 or subsequent legislation (e.g. any recorded information that relates to a "Service User" who is also an identified or identifiable living individual).

- "Relationship Data". This means any recorded information that describes (or infers) a relationship between a "Service User", "Identity Provider" or "Service Provider" with another "Service User", "Identity Provider" or "Service Provider" and includes any cookie or program whose purpose is to supply a means through which relationship data are collected.

3. Other terms used in relation to the Principles are defined as follows:

- "Identity Assurance Service". This includes relevant applications of the technology (e.g. hardware, software, database, documentation) in the possession or control of any "Service User", "Identity Provider" or "Service

18 Note: the text of Schedule 13A is lifted from https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles). It is open to Parliament.

Provider" that is used to facilitate identity assurance activities; it also includes any IdA Data processed by that technology or by an Identity Provider or by a Service Provider in the context of the Service; and any IdA Data processed by the underlying infrastructure for the purpose of delivering the IdA service or associated billing, management, audit and fraud prevention.

- "Identity Provider". This means the certified individual or certified organisation that provides an Identity Assurance Service (e.g. establishing an identity, verification of identity); it includes any agent of a certified Identity Provider that processes IdA data in connection with that Identity Assurance Service.

- "Participant". This means any "Identity Provider", "Service Provider" or "Service User" in an Identity Assurance Service. A "Participant" includes any agent by definition.

- "Processing". In the context of IdA data means "collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, correlating, aggregating, accessing" the data and includes any other operation performed on IdA data.

- "Provider". Includes both "Identity Provider" and/or "Service Provider".

- "Service Provider". This means the certified individual or certified organisation that provides a service that uses an Identity Provider in order to verify identity of the Service User; it includes any agent of the Service Provider that processes IdA data from an Identity Assurance Service.

- "Service User". This means the person (i.e. an organisation (incorporated or not) or an individual (dead or alive) who has established (or is establishing) an identity with an Identity Provider; it includes an agent (e.g. a solicitor, family member) who acts on behalf of a Service User with proper authority (e.g. a public guardian, or a Director of a company, or someone who possesses power of attorney). The person may be living or deceased (the identity may still need to be used once its owner is dead, for example by an executor).

- "Third Party". This means any person (i.e. any organisation or individual) who is not a "Participant" (e.g. the police or a Regulator). Note: we think it helpful to create a link to the language from the National Strategy for Trusted Identities in Cyberspace (NSTIC) which defines participants as "the collective subjects, identity providers, attribute providers, relying parties, and identity media taking part in a given transaction". This way, Third Parties are not Participants.

Part 2: The Nine Identity Assurance Principles

Any exemptions from these Principles must be specified via the "Exceptional Circumstances Principle. (See Principle 9).

1. User Control Principle

Statement of Principle: "I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them."

1.1 An Identity Provider or Service Provider must ensure any collection, use or disclosure of IdA data in, or from, an Identity Assurance Service is approved by each particular Service User who is connected with the IdA data.

1.2 There should be no compulsion to use the Identity Assurance Service and Service Providers should offer alternative mechanisms to access their services. Failing to do so would undermine the consensual nature of the service.

2. **Transparency Principle**

Statement of Principle: "Identity assurance can only take place in ways I understand and when I am fully informed."

2.1 Each Identity Provider or Service Provider must be able to justify to Service Users why their IdA data are processed. Ensuring transparency of activity and effective oversight through auditing and other activities inspires public trust and confidence in how their details are used.

2.2 Each Service User must be offered a clear description about the processing of IdA data in advance of any processing. Identity Providers must be transparent with users about their particular models for service provision.

2.3 The information provided includes a clear explanation of why any specific information has to be provided by the Service User (e.g. in order that a particular level of identity assurance can be obtained) and identifies any obligation on the part of the Service User (e.g. in relation to the User's role in securing his/her own identity information).

2.4 The Service User will be able to identify which Service Provider they are using at any given time.

2.5 Any subsequent and significant change to the processing arrangements that have been previously described to a Service User requires the prior consent or approval of that Service User before it comes into effect.

2.6 All procedures, including those involved with security, should be should be made publicly available at the appropriate time, unless such transparency presents a security or privacy risk. For example, the standards of encryption can be identified without jeopardy to the encryption keys being used.

3. Multiplicity Principle

Statement of Principle: "I can use and choose as many different identifiers or identity providers as I want to."

3.1 A Service User is free to use any number of identifiers that each uniquely identifies the individual or business concerned.

3.2 A Service User can use any of his identities established with an Identity Provider with any Service Provider.

3.3 A Service User shall not be obliged to use any Identity Provider or Service Provider not chosen by that Service User; however, a Service Provider can require the Service User to provide a specific level of Identity Assurance, appropriate to the Service User's request to a Service Provider.

3.4 A Service User can choose any number of Identity Providers and where possible can choose between Service Providers in order to meet his or her diverse needs. Where a Service User chooses to register with more than one Identity Provider, Identity Providers and Service Providers must not link the

Service User's different accounts or gain information about their use of other Providers.

3.5 A Service User can terminate, suspend or change Identity Provider and where possible can choose between Service Providers at any time

3.6 A Service Provider does not know the identity of the Identity Provider used by a Service User to verify an identity in relation to a specific service. The Service Provider knows that the Identity Provider can be trusted because the Identity Provider has been certified, as set out in GPG43 – Requirements for Secure Delivery of Online Public Services (RSDOPS).

4. Data Minimisation Principle

Statement of Principle: "My interactions only use the minimum data necessary to meet my needs."

1 Identity Assurance should only be used where a need has been established and only to the appropriate minimum level of assurance.

2 Identity Assurance data processed by an Identity Provider or a Service Provider to facilitate a request of a Service User must be the minimum necessary in order to fulfil that request in a secure and auditable manner.

3 When a Service User stops using a particular Identity Provider, their data should be deleted. Data should be retained only where required for specific targeted fraud, security or other criminal investigation purposes.

5. Data Quality Principle

Statement of Principle: "I choose when to update my records."

5.1 Service Providers should enable Service Users (or authorised persons, such as the holder of a Power of Attorney) to be able to update their own personal data, at a time at their choosing, free of charge and in a simple and easy manner.

5.2 Identity Providers and Service Providers must take account of the appropriate level of identity assurance required before allowing any updating of personal

data.

6. Service User Access and Portability Principle

Statement of Principle: "I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want."

6.1 Each Identity Provider or Service Provider must allow, promptly, on request and free of charge, each Service User access to any IdA data that relates to that Service User.

6.2 It shall be unlawful to make it a condition of doing anything in relation to a Service User to request or require that Service User to request IdA data.

6.3 The Service User must be able to require an Identity Provider to transfer his personal data, to a second Identity Provider in a standard electronic format, free of charge and without impediment or delay.

7. **Certification Principle**

Statement of Principle: "I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements."

7.1 As a baseline control, all Identity Providers and Service Providers will be certified against a shared standard. This is one important way of building trust and confidence in the service.

7.2 As part of the certification process, Identity Providers and Service Providers are obliged to co-operate with the independent Third Party and accept their impartial determination and to ensure that contractual arrangements:

- reinforce the application of the Identity Assurance Principles
- contain a reference to the independent Third Party as a mechanism for dispute resolution

7.3 There will be a certification procedure subject to an effective independent audit regime that ensures all relevant, recognised identity assurance and

technical standards, data protection or other legal requirements, are maintained by Identity Providers and Service Providers.

7.4 In the context of personal data, certification procedures include the use of Privacy Impact Assessments, Security Risk Assessments, Privacy by Design concepts and, in the context of information security, a commitment to using appropriate technical measures (e.g. encryption) and ever improving security management. Wherever possible, such certification processes and security procedures reliant on technical devices should be made publicly available at the appropriate time.

7.5 All Identity Providers and Service Providers will take all reasonable steps to ensure that a Third Party cannot capture IdA data that confirms (or infers) the existence of relationship between any Participant. No relationships between parties or records should be established without the consent of the Service User.

7.6 Certification can be revoked if there is significant non-compliance with any Identity Assurance Principle.

8. Dispute Resolution Principle

Statement of Principle: "If I have a dispute, I can go to an independent Third Party for a resolution."

8.1 A Service User who, after a reasonable time, cannot, or is unable, to resolve a complaint or problem directly with an Identity Provider or Service Provider can call upon an independent Third Party to seek resolution of the issue. This could happen for example where there is a disagreement between the Service User and the Identity Provider about the accuracy of data.

8.2 The independent Third Party can resolve the same or similar complaints affecting a group of Service Users.

8.3 The independent Third Party can co-operate with other regulators in order to resolve problems and can raise relevant issues of importance concerning the Identity Assurance Service.

8.4 An adjudication/recommendation of the independent Third Party should be published. The independent Third Party must operate transparently, but detailed

case histories should only be published subject to appropriate review and consent.

8.5 There can be more than one independent Third Party.

8.6 The independent Third Party can recommend changes to standards or certification procedures or that an Identity Provider or Service Provider should lose their certification.

9. Exceptional Circumstances Principle

Statement of Principle: "Any exception has to be approved by Parliament and is subject to independent scrutiny."

9.1 Any exemption from the application of any of the above Principles to IdA data shall only be lawful if it is linked to a statutory framework that legitimises all Identity Assurance Services, or an Identity Assurance Service in the context of a specific service. In the absence of such a legal framework then alternative measures must be taken to ensure, transparency, scrutiny and accountability for any exceptions.

9.2 Any exemption from the application of any of the above Principles that relates to the processing of personal data must also be necessary and justifiable in terms of one of the criteria in Article 8(2) of the European Convention of Human Rights: namely in the interests of national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals, or for the protection of the rights and freedoms of others.

9.3 Any subsequent processing of personal data by any Third Party who has obtained such data in exceptional circumstances (as identified by Article 8(2) above) must be the minimum necessary to achieve that (or another) exceptional circumstance.

9.4 Any exceptional circumstance involving the processing of personal data must be subject to a Privacy Impact Assessment by all relevant "data controllers" (where "data controller" takes its meaning from the Data Protection Act).

9.5 Any exemption from the application of any of the above Principles in relation to IdA data shall remain subject to the Dispute Resolution Principle.