Data Protection and Digital Information (No.2) Bill

Law Society of Scotland – briefing for Second Reading

April 2023

Introduction

The Law Society of Scotland is the professional body for over 12,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied, and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom Governments, Parliaments, wider stakeholders, and our membership.

We previously responded to the Department for Digital, Culture, Media & Sport's consultation *Data: a new direction*[1] in November 2021.

We now welcome the opportunity to consider and provide comment on the Data Protection and Digital Information (No. 2) Bill (The Bill) ahead of the second reading of the Bill in the House of Commons on 17 April 2023[2].

General remarks

The Bill seeks to update and simplify the United Kingdom's data protection framework under The Data Protection Act 2018, and the UK General Data Protection Regulation, following the UK's exit from the European Union, and the Bill intends to reduce burdens on organisations whilst ensuring high data protection standards and the Bill will amend some of the provisions in the current data protection legislation.

The Government considers that, "[3]some elements of current data protection legislation - the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA) 2018 - create barriers, uncertainty and unnecessary burdens for businesses and consumers".

[1] uk-digital-id-trust-framework-law-society-of-scotland.pdf (lawscot.org.uk)

[2] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/220265v2.pdf

[3] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265en.pdf

The Bill proposes to give organisations greater flexibility on how they can comply with certain parts of the data protection legislation, improving the clarity of the data protection framework, notably for research organisations and the Bill seeks to provide greater certainty for cross-border flows of personal data. In addition, the Bill seeks to extend data sharing powers under section 35 of the Digital Economy Act 2017 which will include businesses.

The Bill proposes to reform the Information Commissioner, namely its governance structure, duties, enforcement powers, reporting requirements, complaints processes and its development of statutory codes of practice.

The Government states that under the current data protection legislation regarding the role of the Information Commissioner, "[4]does not provide the Information Commissioner with a sufficiently clear framework of objectives and duties in relation to its data protection responsibilities, against which to prioritise its activities and resources, evaluate its performance and be held accountable by its stakeholders".

The Bill seeks to change the role of the Information Commissioner, as the Bill proposes to move the focus of the Commissioner to help organisations comply with the law from the outset and the Bill proposes to create new duties for the Commissioner to have regard to competition, economic growth, and innovation.

Furthermore, the Bill seeks to create a system for the provision of digital verification services in the UK, to ensure that the digital verification services are reliable and that digital identities have the same certification and trust as paper documentation.

The Bill proposes that law enforcement and national security agencies can use personal data can for the purposes of law enforcement and national security, where this is in the public interest.

The Bill also proposes to amend the Privacy and Electronic Communications Regulations 2003, relating to confidentiality of terminal equipment (such as cookie rules), unsolicited direct marketing communications (such as nuisance calls), and communications security (such as, network traffic and location data).

The Bill seeks to amend Part 3 of The Data Protection Act 2018 by proposing to introduce a definition of consent which has an equivalent meaning in other regimes, by creating codes of conduct and introducing similar exemptions for legal professional privilege and by protecting level privilege.

Furthermore, the Bill proposed to amend Part 3 of the Data Protection Act 2018 by removing the requirement for competent authorities to inform the data subject that they have been subject to automated decision making if certain conditions are met.

[4] https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265en.pdf

Whilst the Bill seeks to amend the United Kingdom's data protection framework under The Data Protection Act 2018, and the UK General Data Protection Regulation, we have concerns regarding some of the reforms the Bill proposes, as the Bill will lead to two systems of data regulation in Europe, as organisations who process or store data in Europe, are still required to comply with the requirements and obligations of the Regulation (EU) 2016/679 General Data Protection Regulations. We believe that this may lead to confusion to organisations operating across different boundaries.

We consider the Bill provides the Government with the opportunity to have one single, standalone, and clear piece of data protection legislation following the United Kingdom's withdrawal from the European Union. We are concerned that the Bill will mean that data protection law in the UK is now contained over three main sources, namely the Bill, UK GDPR and the Data Protection 2018 Act, which may cause confusion for parties and organisations.

Comments on the Bill

The Bill is divided into six parts and has thirteen schedules.

Part 1 and Schedule 1, 2, 3, 4, 5, 6, 7 (Part 1) & (Part 2), 8, 9,

This Part contains the key definitions in the Bill.

Clause 1 (1) of the Bill (information relating to an identifiable living individual), amends section 3 (3) of the Data Protection Act 2018, by confirming that a living individual may be identifiable either directly or indirectly.

Clause 1 (2) of the Bill adds a new section to section 3A of the Data Protection Act 2018, as under section 3A(1)-(3) information being processed is information relating to an identifiable living individual, where, the living individual is identifiable by the controller or processor by reasonable means at the time of the processing. Secondly, where, where the controller or processor knows, or ought reasonably to know, that— (a) another person will, or is likely to, obtain the information as a result of the processing, and (b) the living individual will be, or is likely to be, identifiable by that person by reasonable means at the time of the processing.

We feel that the explanation of reasonable means under clause 1 (2), namely an individual is identifiable by a person "by reasonable means" if the individual is identifiable by the person by any means that the person is reasonably likely to use, is too narrow, complicated and is not very clear.

Clauses 5 and 6 sets out the data protection principles.

We note the proposal under clause 7 (vexatious or excessive requests by data subjects) changes the threshold for responding to data subject requests, and the Bill uses similar terminology as in Freedom of Information legislation, and we consider that the Bill should define vexatious, and use similar to definitions to guidance from the Information Commissioner, namely '[5]manifestly unjustified, inappropriate or improper use of a formal procedure'.

Clause 8 to 10 contains the provisions of data subject's rights, including, the time limits for responding to requests by data subjects (clause 8), information to be provided to data subjects (clause 9), and clause 10 set out data subjects' rights to information – the legal professional privilege exemption in relation to law enforcement processing.

We note Clause 11 regarding automated decision making and note that the Bill will remove the right not to be subject to automated decision making and replaces it with a right to human intervention in relation to significant decisions. Clause 11 amends Article 22 of the UK GDPR with a new Article 22A-D. We consider that Article 22 of the UK GDPR provides important and essential safeguards for individuals subjected to automated decision making which has an impact on their lives. Individuals must be able to understand what is happening to them and why and they must be able to challenge this to ensure public trust. The Equalities and Human Rights Commission published a paper[6] in September 2022 outlining concerns about AI and discrimination in the public sector. We are of the view that these protections should be strengthened, and this is likely to depend on the definition of 'significant'. This could threaten the UK's adequacy with the EU. We also wish to highlight the article from the ICO investigation into the use of AI and automated decision-making in benefits administration by local authorities[7]. We note that there are amendments providing protections when special category data is used. We are not sure about the logic of restricting the protection in this way to when special category personal data is being used.

Furthermore, and with similar concerns in relation to adequacy, we note clause 13 concerning the removal of the requirement to appoint a representative for controllers etc outside the UK, and that Article 27 of the UK GDPR (representatives of controllers or processors not established in the United Kingdom (clause 14 (1) has been omitted.

We note clause 14, the senior responsible individual, which replaces the requirements on Data Protection Officers in Articles 37 to 39 of the UK GDPR and sections 69 to 71 of the Data Protection Act 2018, as data controllers and processors must designate one individual to be its senior responsible individual (14 (1), who must be part of the organisation's senior management (14 (3) (a) or this role can be designated to other individual(s) within the organisation's senior management (14 (3) (b). We feel that this may be

[5] What does vexatious mean? | ICO

[6] https://www.equalityhumanrights.com/en/our-work/news/equality-watchdog-takes-action-address-discrimination-use-artificial-intelligence

[7] Blog: Addressing concerns on the use of AI by local authorities | ICO

onerous for businesses and organisations, as senior managers may not have the expert knowledge as Data Protection Officers have or capacity to perform this role. They may also have a conflict of interest, which is excluded by the requirements of the GDPR in relation to DPOs.

We feel that the assessment of high-risk processing under clause 17, which amends Article 35 of the UK GDPR and section 64 of the Data Protection Act 2018 is leaner and less prescriptive, as clause 17 (2) amends Article 35 of the UK GDPR from Data Protection Impact Assessments to Assessments of high-risk processing. We are not sure that there is a significant difference but welcome the retention of a risk assessment as we view that as important.

We note clause 21 which concerns international transfers of personal data, as clause 21 inserts Schedules 5, 6, and 7, which amend Chapter 5 of the UK GDPR and Chapter 5 of Part 3 of the Data Protection Act 2018 to reform the UK's regime for international transfers of personal data. The biggest challenge for smaller organisations has been carrying out risk assessments in relation to the country data is being transferred to. Although it seems sensible to make this process easier, it risks the UK's adequacy decision.

Furthermore, we have concerns regarding the provisions of Schedule 5, Article 44A (2) (a), which allows the Secretary of State to approve the transfers of personal data to a third country or an international organisation by regulation, rather than by general principles or adequacy decisions, as will also risk the UK's adequacy. Onward transfers from the UK were one of the concerns raised when the EU was considering the original adequacy decision.

Clauses 22 and 23 set out the safeguards for processing for research etc purposes. We have some concerns about the proposals regarding research. Currently, medical research already has significant levels of regulation which are effective in both allowing research to take place and protecting individuals' privacy rights, and we are unconvinced of the need to significantly change these existing regulations.

Clause 24 sets out the national security exemption, and clauses 25 and 26 concern intelligence services, namely the joint processing by intelligence services and competent authorities (clause 25).

Clauses 27 to 33 set out the role of the Information Commissioner.

We are concerned with the proposals in the Bill which impact on the independence of the Information Commissioner. Clause 27 sets out the duties of the Commissioner in carrying out their functions, this amends Part 5 of the Data Protection Act 2018 by inserting new sections providing for a principal objective and general duties for the Commissioner when carrying out functions.

Under clause 28 (2), The Secretary of State may designate a statement as the statement of the government's strategic priorities on data protection (under s. 120E (1) & (2) of the Data Protection Act 2018) and The Commissioner must have regard to the statement of strategic priorities when carrying out functions under the Bill (s. 120F (1) Data Protection Act 2018). We feel as the regulator, whilst the Information Commissioner will have regard to the government's priorities, the role as regulator has to be impartial and objective in carrying out their functions.

We are also concerned that the Information Commissioner and non-executive members are to be appointed by the Secretary of State (under Schedule 12A) and the Information Commissioner (under clause 29 (2) of the Bill and inserted by s. 124A (1) of the Data Protection Act 2018), must prepare appropriate codes of practice giving guidance as to good practice in the processing of personal data (if required to do so) by regulations made by the Secretary of State, thus impacting the independence of the Commissioner.

Clause 32 concerns vexatious or excessive requests made to the Information Commissioner and analysis of performance is determined under clause 33.

The Information Commissioner's enforcement powers are set out in clauses 34 to 42. The Information Commissioner can require documentation (clause 34), and the Commissioner can require a report (clause 35). Interview notices are set in clause 36, whereas clause 37 concerns penalty notices and the requirement for the Commissioner to produce an annual report on regulatory action (clause 38). We support these practical proposals.

We support the proposal of the complaints process under clause 39 (complaints to controllers), whereby data controllers, such as organisations must facilitate and take appropriate steps to respond to a complaint from a data subject and inform the complainer of the outcome of the complaint (clause 39 (4). We think this proposal makes sense, rather than complaints being directly sent to the Information Commissioner, as data controllers should have the opportunity to investigate a complaint and respond to a complaint in the first instance. In practice this is what is happening currently.

Clause 39 concerns complaints to controllers and clause 40 sets out the power of the Commissioner to refuse an act on certain complaints. Clause 41 concerns complaints of minor and consequential amendments and clause 42 sets out the consequential amendments to the EITSET Regulations.

Clause 43 sets out the protection of prohibitions and restrictions on processing personal data.

Part 2

This Part concerns Digital Verification Services. We have no comments.

Part 3

This Part concerns Customer Data and Business Data.

We note the provisions on Smart Data in Part 3, which includes provisions for the Secretary of State, or the Treasury may by regulations to impose fees on data holders and others (Clause 70) and to impose a levy on data holders and have no comments.

Part 4 and Schedule 10, 11 (Part 1) & (Part 2), 12

This Part concerns other provision(s) about digital information, as clauses 78 to 86 deal with privacy and digital information, including electronic communication.

We note clause 79 regarding storing information in the terminal equipment of a subscriber or user, as this allows cookies to be used for a broader range of activities without consent. We do not support the requirement for prior consent being removed for all types of cookies, as some types of cookies are extremely invasive allowing large organisations to gather information about a user across platforms and devices and when these technologies are explained to individuals most find their use concerning. Inferred data is personal data and its uses are damaging to public consent more broadly.

We do believe however that first party analytics cookies where mostly personal data is being used to inform the website operator only who is looking at their websites should not require consent, and in our opinion, this is non-invasive and very valuable for organisations, however we are concerned that there could end up being a different approach taken in the EU. Cognisance of the new ePrivacy Regulation as it progresses.

We are concerned about clause 82 (3) (a) regarding the use of electronic mail for direct marketing purposes, as a person can use direct marketing for the purpose of furthering a charitable, political, or other non-commercial objective. Whilst we support the use of direct marketing for charitable and other non-commercial objectives, we have concerns about relaxing the rules around the use of direct marketing for political purposes and the use of direct marketing for political purposes should be removed or tightened.

Trust services are set out in clauses 87 to 91 and clauses 92 and 93 concern data sharing.

We note the contents of clause 89 regarding the Removal of recognition of EU standards. This permits the Secretary of State by regulations under clause 89(1)(a) to remove all qualifiers from a qualified electronic signature. We consider that this reduces the benefit of the qualified electronic signature. Under clause 89(1)(b), the revocation of Article 24A of the eIDAS Regulation (recognition of EU standards etc for qualified trust services) essentially disallows qualified electronic signatures.

Part 5 and Schedule 13

This Part concerns Regulation and Oversight.

We note clause 101 (the abolition of the office of Information Commissioner) and we are concerned that this and what could be seen as a dilution to the independence of the supervisory authority may result in the loss of the Adequacy decision. We are unaware of any evidence to suggest why the Commissioner's role is to be abolished and why these changes have been included given Article 51 of the EU GDPR.

We also note clause 103 regarding the Transfer of property etc to the Information Commission, where the Secretary of State can transfer property, rights and liabilities from the Information Commissioner to the Information Commission (clause 103 (1). The transfer scheme can include the continuation of things in the process and TUPE rights amongst others.

Part 6

Part 6 of the Bill concerns the final provisions. We have no comments.

For further information, please contact:

Gavin Davies
Policy Team
Law Society of Scotland
DD: 0131 370 1985
GavinDavies@lawscot.org.uk