Law Society of Scotland

Written evidence

Law Society of Scotland briefing on the Data Protection Bill

March 2018

Introduction

The Law Society of Scotland is the professional body for over 11,000 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.

The Society's Privacy Law and Immigration Law Sub-committees have considered the Data Protection Bill[1] and welcome the opportunity to respond to the Public Bill Committee's call for evidence. The Sub-committees would like to put forward the following comments for consideration.

General Remarks

UK withdrawal from the EU

We continue to emphasise[2] the importance of ensuring continued data flows between the UK and the EU following withdrawal. We outlined our concerns about relying on an adequacy decision to ensure that data continued to be transferable between the UK and EU. We consider that it would be preferable to have a specific agreement in place to cover exchange of personal data between the UK and EU following withdrawal. However, if this is not achieved within the timescale of the withdrawal negotiations an adequacy designation could provide a helpful interim solution.

We also commented on the likelihood of achieving adequacy and outlined a number of associated concerns, including the weakening of UK citizens' rights in an EU context post withdrawal. In addition we highlighted the increasing importance to UK businesses of facilitating flows of personal data and the critical

[1] https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf

[2] See previous briefing from October 2017 at Annex 2, also available at https://www.lawscot.org.uk/media/359224/law-society-of-scotland-briefing_data-protection-and-eu-withdrawal_oct-2017.pdf

importance of UK companies being eligible to process personal data originating in the EU. Understanding how the UK will designate "adequacy" of others is important, but is not the sole issue.

Legal certainty

We have serious concerns regarding the clarity and accessibility of the bill.

It is central to the rule of law that people should be able to ascertain their rights and obligations and therefore they must know that the rules are. This goes beyond access to the legislation itself to a reasonable expectation that citizens will be able to understand the text sufficiently to apply it to their own lives. As has been noted by Lord Simon of Glaisdale, it is a "derogation from the right of a citizen"[3] if legislation cannot be understood.

We have serious concerns regarding the drafting of the Bill, which contains such a high volume of references to the GDPR as to be almost incomprehensible. Furthermore, the format of the Bill does not follow that of the GDPR, thereby exacerbating the problems of interpreting the Bill while cross-referring to the text of the GDPR. We do not consider that the Bill is accessible even to lawyers who specialise in this area and therefore consider that it fails to offer the requisite clarity and accessibility.

Comments on specific provisions

Clause 10 – Special categories of personal data and criminal convictions etc data

Clause 10 relates to special categories of personal data which are particularly sensitive. Clause 10(6) gives the Secretary of State the power to amend conditions and safeguards under Schedule 1. However, we consider that any changes should be subject to proper parliamentary scrutiny. Following UK withdrawal from the EU, such changes could take us out of line with the GDPR and thereby risk undermining any adequacy designation. However, if the clause were amended to allow the Secretary of State to make amendments in order to update UK law to maintain alignment with EU law, this could be useful if an adequacy decision is successfully obtained.

Clause 16 – Power to make further exemptions etc by regulations

We do not consider it is appropriate for the clause 16 powers to be held by the Secretary of State. As set out above this would allow the Secretary of State to change the law without requisite scrutiny.

[3] GC Thornton, Legislative Drafting (4th edn Butterworths, London, 1996) p50

We are aware that a number of other parties have raised similar concerns. For example the BMA has a particular concern that the clause "would give the Government an inappropriate, fast-track power to change the law, through secondary legislation, on how confidential health data are shared, with little scrutiny or oversight. Significantly, the House of Lords' secondary legislation scrutiny committee has also warned that delegations of power in clause [16] "*are inappropriately wide*" and they "*recommend their removal from the Bill*"."[4]

Furthermore such changes could result in either convergence with, or divergence from, EU law in the future. Modification under delegated legislation should only be possible where necessary to maintain the compatibility of UK law with the GDPR post Brexit in order to ensure the UK is eligible for adequacy status, unless another mechanism for flows of data between the UK and EU is agreed. Further information on adequacy and the importance of data flows can be found in our briefing from October 2017[5] (see Annex 2).

Clause 18 – Transfers of personal data to third countries etc

We note that references to a third country and adequacy decision under Article 45(3) of the GDPR will cease to make sense once the UK leaves the EU. The Act will need to be amended upon withdrawal to make necessary changes.

Clause 22 – Application of the GDPR to processing to which this Chapter applies

The wording of clause 22(1) is confusing. It would be preferable to say that the GDPR applies in the UK as if it were an act of the UK parliament extending to England and Wales, Scotland, and Northern Ireland and that reference to "articles" was amended to "sections" (see Annex 1).

2(2) and (3) appear to be circular definitions and are likely to cause confusion.

Ensuring compatibility with the GDPR

While we raise concerns about wide discretionary powers which the Bill as currently drafted would give to the Secretary of State, we consider that a limited power to ensure ongoing compatibility with the GDPR could be helpful if no specific agreement on data is concluded prior to withdrawal and an adequacy

[4] https://www.bma.org.uk/-/.../bma-briefing-data-protection-bill-report-stage.pdf?la=en

[5] https://www.lawscot.org.uk/media/359224/law-society-of-scotland-briefing_data-protection-and-eu-withdrawal_oct-2017.pdf

decision is sought. This would be similar to the provision in clause 180 which gives the Secretary of State the power to reflect changes to the Data Protection Convention.

We therefore suggest a new clause is inserted after s.180 follows:

"**s181 Power to reflect changes to the GDPR**

(1) The Secretary of State shall by regulations make such provision as the Secretary of State considers necessary in connection with the interpretation of the GDPR by the Institutions of the European Union or an amendment of, or an instrument replacing, the GDPR in order to ensure that the data protection laws of the United Kingdom remain fully compatible with the GDPR,
(2) The power under subsection (1) includes power—
(a) to add to or otherwise amend the Commissioner's functions, and
(b) to amend this Act.
(3) Regulations under this section are subject to the affirmative resolution procedure."

It could also be appropriate to consider a time limit for this clause.

Schedule 2, Paragraph 4 – Immigration

This paragraph contains an exemption from a number of rights, including the right to make a subject access request (SAR), for "the maintenance of effective immigration control, or…the investigation or detection of activities that would undermine the maintenance of effective immigration control."

The exemption has been defended by the Culture Minister as ensuring that 'a minority of individuals cannot abuse data protection law with the sole intent of undermining immigration controls.'[6]

However, we do not consider that such a broad exemption is appropriate unless divulging the information would damage investigation or enforcement. In the first instance, we are not aware of any particular problem with abuse of data protection law by migrants. We consider that a narrower, more targeted exemption would be more appropriate if a specific problem has been identified. We are not in a position to suggest an alternative approach without further information as to the abuse the Government is trying to target.

[6] Matt Hancock - https://hansard.parliament.uk/Commons/2018-03-05/debates/0343F7DB-6456-4448-B9B8-BA7A1FFCD01D/DataProtectionBill(Lords)#contribution-15C5D5B1-4963-48D7-84A6-DECAD6629BCB

Practitioners note that they make use of SARs[7] to obtain a copy of the Home Office file when preparing an application. Often a client has no idea what previous applications have been made on their behalf and has not kept a copy of decision letters. A mandate to any previous agents and an SAR may therefore be the only way of finding out their immigration history.[8] Where Home Office records are incorrect, the process also allows for correction of inaccurate information.

Furthermore the SAR is particularly important in the context of applications which require continuous lawful residence (for instance an application for indefinite leave to remain (ILR) after 10 years' continuous lawful residence). In order to determine whether an applicant qualifies it is necessary to determine when all previous applications for further leave were submitted as if any were submitted after expiry of the person's existing leave, they have overstayed and broken continuous residence (although there are exceptions). Clients who have made previous applications by themselves often do not keep copies of the application form or documents sent. They may not have intended to stay for 10 years originally and therefore have failed to retain a record of applications as they did not anticipate making an ILR application at a later date. Sometimes people are simply disorganised. Without the ability to submit a SAR people in this situation would have no way to determine if they meet the requirements or not. They would simply need to make an application (paying the £2,297 fee) and hope for the best. The ability to make SARs is therefore an important mechanism in ensuring access to justice in an immigration context.

Schedule 2, paragraph 17 – Legal professional privilege

and

Schedule 11, Paragraph 9 – Legal professional privilege

These two paragraphs are drafted in almost identical terms. However, we are concerned that they seem to equate legal professional privilege with the ethical obligation of confidentiality.

[7] The Home Office requires certification of ID by a solicitor or immigration adviser before a SAR will be accepted the Home Office. This has already made it much more difficult for unrepresented migrants to submit a SAR.

[8] Other stakeholders have raised similar concerns including the Bar Council (http://www.barcouncil.org.uk/media/641717/180228_immigration_control_exemption_hoc_2r_briefing_data_protection_bill_bar_council.pdf), the Law Society of England and Wales (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/memo/dpb20.pdf) and the Immigration Law Practitioners' Association (https://publications.parliament.uk/pa/cm201719/cmpublic/DataProtection/memo/dpb16.pdf)

Legal professional privilege is recognised in Scotland as a matter of law, although it is not identical to the concept as understood in England and Wales.[9] It is a matter of the rules of evidence and also a fundamental human right.

Similarly, an ethical obligation of confidentiality is imposed upon regulated lawyers in all UK jurisdictions. In Scotland, solicitors are bound by the duty of confidentiality in terms of the Society's practice rules.

The exemption should therefore recognise both concepts as these are central to access to justice and to ensuring open communications between lawyers and their clients.

We propose amendment to Schedule 2, paragraph 17 and Schedule 11, paragraph 9 to read as follows:

"Legal professional privilege

[x] The listed [GDPR] provisions do not apply to personal data that consists of information which is protected by legal professional privilege or the duty of confidentiality."

See further suggested amendments in Annex 1.

Schedule 15, paragraph 11 – Matters exempt from inspection and seizure: privileged communications

Paragraph 11 purports to exempt privileged material from searches, as one would expect. However, we are concerned that the paragraph 11(1) and (2) as currently drafted protect only advice in relation to obligations, liabilities or rights under the data protection legislation or in connection with or in contemplation of proceedings under or arising out of that legislation. It therefore narrows the usual scope of privilege considerably. We emphasise that privilege should attach to communications between a legal adviser and their client, regardless of the subject matter of those communications.

While in this context it is anticipated that the ICO would only seek a warrant in connection with data protection matters, there is a risk that other privileged material could therefore be caught up in the process. For example if the ICO was investigating a data brief involving staff matters, a warrant might be secured to recover documents relating to those staff members over a certain period. As part of that investigation, the ICO might collect documents form the company's lawyers regarding a separate litigation matter. Those

[9] See *R. (on the application of Prudential Plc)* v *Special Commissioner of Income Tax* [2013] UKSC 1, Lord Reed at paras 103-113

documents would be privileged and should remain privileged but paragraph 11, as currently drafted, would mean that the privilege could be lost.

The references to communications relating to advice "under the data protection legislation" should therefore be removed to ensure privilege of all communications is recognised.

Schedule 6, paragraph 4 – References to the Union and to Member States

Schedule 6 Part 1 deals with modifications to the applied GDPR. Paragraph 6(4) reads as follow: "References to "the Union", "a Member State" and "Member States" have effect as references to the United Kingdom". There a number of references, eg Article 1(3), in the GDPR which refer to "the free movement of personal data within the Union". However "free movement" is a specific European Union concept so reference to "free movement of data within the United Kingdom" does not make sense, particularly as data protection is a reserved matter and data protection law applies across the UK.

Schedule 15, paragraph 5 – Content of warrants

Paragraph 5 seems to give powers to operate and test equipment (eg a laptop or computer) but not to seize the equipment to allow those tests to be carried out off site and to prevent, eg deletion of relevant material. However, it is possible that hardware could be caught within the definition of "material" under 2(a). A definition of "material" is therefore required to ensure clarity of the legislation.

Schedule 15, paragraph 12 – Parliamentary privilege

There may also be a question as to whether, in light of the privileged status in law conferred on the Scottish Parliament under s.40 of the Scotland Act 1998, the Data Protection Bill should grant privilege, or some measure of privilege, to the Scottish Parliament also.

For further information, please contact:
Carolyn Thurston Smith
Policy Team
Law Society of Scotland
DD: (+44)(0)131 476 8205
carolynthurstonsmith@lawscot.org.uk

Annex 1A: Amendments to be moved at Committee Stage

DATA PROTECTION BILL

AMENDMENTS TO BE MOVED AT COMMITTEE STAGE

Clause 10, page 6, line 19, leave out subsections (6) and (7)

Clause 16, page 9, line 12, leave out clause 16

Clause 22, page 13, line 20, leave out “but”

Clause 22, page 13, line 20, leave out “part” and insert

“sections”

Schedule 2, page 146, line 41, leave out paragraph 17 and insert

“17 The listed GDPR provisions do not apply to personal data that consists of information which is protected by legal professional privilege or the duty of confidentiality.”

Schedule 11, page 189, line 17, leave out paragraph 9 and insert:

“9 The listed provisions do not apply to personal data that consists of information which is protected by legal professional privilege or the duty of confidentiality.”

Schedule 15, page 201, line 6, leave out “with respect to obligations, liabilities or rights under the data protection legislation”

Schedule 15, page 201, line 14, leave out “under or arising out of the data protection legislation and (c) for the purposes of such proceedings”

Annex 1B: Amendments to be moved at Committee stage with reasons and effects

DATA PROTECTION BILL

AMENDMENT TO BE MOVED AT COMMITTEE STAGE

Clause 10, page 6, line 19, leave out subsections (6) and (7)

Effect

The effect of this amendment is to remove the power of the Secretary of State to add, vary or omit conditions or safeguards by regulations.

Reason

We consider that any changes to conditions or safeguards should be subject to proper parliamentary scrutiny.

Furthermore, following UK withdrawal from the EU, such changes could take us out of line with the GDPR and thereby risk undermining any adequacy designation: amendment could therefore have wider consequences. This reinforces the need for parliamentary scrutiny of any proposed changes.

Law Society of Scotland

DATA PROTECTION BILL

AMENDMENT TO BE MOVED AT COMMITTEE STAGE

Clause 16, page 9, line 12, leave out clause 16

Effect

The effect of this amendment is to remove the power of the Secretary of State to add, vary or omit exemptions in Schedules 2 to 4.

Reason

We consider that any changes to the exemptions in these schedules should be subject to proper parliamentary scrutiny. We do not consider it appropriate for the clause 16 powers to be held by the Secretary of State.

Furthermore, following UK withdrawal from the EU, such changes could take us out of line with the GDPR and thereby risk undermining any adequacy designation: amendment could therefore have wider consequences. This reinforces the need for parliamentary scrutiny of any proposed changes.

Law Society of Scotland

DATA PROTECTION BILL

AMENDMENT TO BE MOVED AT COMMITTEE STAGE

Clause 22, page 13, line 20, leave out “but”

Clause 22, page 13, line 20, leave out “part” and insert

“sections”

Effect

To achieve greater clarity in the bill.

Reason

The wording of clause 22(1) is confusing. It would be preferable to say that the GDPR applies in the UK as if it were an act of the UK parliament extending to England and Wales, Scotland, and Northern Ireland and that reference to “articles” was amended to “sections”.

Law Society of Scotland

DATA PROTECTION BILL

AMENDMENT TO BE MOVED AT COMMITTEE STAGE

Schedule 2, page 146, line 41, leave out paragraph 17 and insert

"17 The listed GDPR provisions do not apply to personal data that consists of information which is protected by legal professional privilege or the duty of confidentiality."

Effect

The effect of this amendment would be to ensure that both privilege and confidentiality are recognised within the legislation.

Reason

Legal professional privilege (LPP) and confidentiality are essential to safeguard the rule of law and the administration of justice. They permit information to be communicated between a lawyer and client without fear of it becoming known to a third party without the clear permission of the client. Many UK statutes already give express protection of LPP and it is vigorously protected by the courts.

The 'iniquity exception' alleviates concerns that LPP may be used to protect communications between a lawyer and client which are being used for a criminal purpose. Such purpose removes the protection from the communications, allowing them to be targeted using existing powers and not breaching LPP.

Law Society of Scotland

DATA PROTECTION BILL

AMENDMENT TO BE MOVED AT COMMITTEE STAGE

Schedule 11, page 189, line 17, leave out paragraph 9 and insert:

"9 The listed provisions do not apply to personal data that consists of information which is protected by legal professional privilege or the duty of confidentiality."

Effect

The effect of this amendment would be to ensure that both privilege and confidentiality are recognised within the legislation.

Reason

Legal professional privilege (LPP) and confidentiality are essential to safeguard the rule of law and the administration of justice. They permit information to be communicated between a lawyer and client without fear of it becoming known to a third party without the clear permission of the client. Many UK statutes already give express protection of LPP and it is vigorously protected by the courts.

The 'iniquity exception' alleviates concerns that LPP may be used to protect communications between a lawyer and client which are being used for a criminal purpose. Such purpose removes the protection from the communications, allowing them to be targeted using existing powers and not breaching LPP.

DATA PROTECTION BILL

AMENDMENT TO BE MOVED AT COMMITTEE STAGE

Schedule 15, page 201, line 6, leave out “with respect to obligations, liabilities or rights under the data protection legislation”

Schedule 15, page 201, line 14, leave out “under or arising out of the data protection legislation and (c) for the purposes of such proceedings”

Effect

The effect of this amendment would be to ensure that the full scope of privilege and is recognised within the legislation and is not confined to advice in relation to obligations, liabilities or rights under the data protection legislation or in contemplation of proceedings under or arising out of that legislation.

Reason

We are concerned that the paragraph 11(1) and (2) as currently drafted protect only advice in relation to obligations, liabilities or rights under the data protection legislation or in connection with or in contemplation of proceedings under or arising out of that legislation. It therefore narrows the usual scope of legal professional privilege (LPP) considerably. We emphasise that privilege should attach to communications between a legal adviser and their client, regardless of the subject matter of those communications.

Legal professional privilege is essential to safeguard the rule of law and the administration of justice. It permits information to be communicated between a lawyer and client without fear of it becoming known to a third party without the clear permission of the client. Many UK statutes already give express protection of LPP and it is vigorously protected by the courts.

The ‘iniquity exception’ alleviates concerns that LPP may be used to protect communications between a lawyer and client which are being used for a criminal purpose. Such purpose removes the protection from the communications, allowing them to be targeted using existing powers and not breaching LPP.

Annex 2 - Law Society of Scotland briefing on the Data Protection Bill and impact of UK withdrawal from the EU, October 2017

Recognition through adequacy decision

There are a number of problems with relying on an adequacy decision as the basis of transfer of data to companies or other business forms in the UK. It would be preferable to have a specific agreement in place to cover exchange of personal data between the UK and EU following withdrawal. However, if this is not achieved within the timescale of the withdrawal negotiations an adequacy designation could provide a helpful interim solution.

It would therefore be helpful to have some information regarding the point at which the UK intends to see an adequacy designation and the anticipated timescales? Is the Government intending to have a designation in place on the date of withdrawal?

Likelihood of achieving adequacy and associated concerns

It would be helpful to have some more information on whether the Government considers that the UK would achieve an adequacy ruling. There is also the linked question of whether other jurisdictions will be regarded as offering a sufficient level of data security to allow transfers of data out of the UK, to both EU and non-EU countries.

Recital 104 refers to 'an adequate level of protection essentially equivalent to that ensured within the Union'. The Information Commissioner has suggested that UK penalties will not increase greatly under the GDPR. This might contrast with the rest of the EU and impact on adequacy.

A number of specific criteria to be considered in assessing adequacy are set out in GDPR Art 45(2)(a). They include consideration of any domestic legislation including that “concerning public security, defence, national security and criminal law and the access of public authorities to personal data as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country…which are complied with in that country...”

The Investigatory Powers Act 2016

In particular concerns have been raised that problems may arise here with the level of access to personal data by public authorities as determined in the Investigatory Powers Act 2016.[10] We are aware that the Act is not yet fully in force but are also of the view that if tested it is unlikely that certain provisions in the Investigatory Powers Act would be found to be acceptable.

In particular we previously identified concerns regarding the requirement for telecommunications operators to retain communications data.[11] Following on from this, in the joined cases C-203/15 and C-698/15 *Tele2 Sverige AB* v *Post-och telestyrelsen* and *Secretary of State for the Home Department* v *Tom Watson & Others* (21 December 2016) the CJEU found that Member States could not pass national legislation requiring general and indiscriminate retention of communications data or location data. There is therefore a risk that the Act may be challenged before the UK withdraws from the EU; even absent such a challenge we consider that as it stands the Act might pose a bar to a finding of adequacy.

It is also unclear as to what extent the Government might consider steps to achieve adequacy if this were indeed to prevent an adequacy finding.

CJEU case law

What impact will there be on adequacy if the UK is not bound by or even bound to have regard to CJEU judgements following withdrawal? Clause 6 of the European Union (Withdrawal) Bill[12] states that decisions of the EU Court will cease to bind UK courts and tribunals following withdrawal:

"6(1) A court or tribunal –

> *(a) is not bound by any principles laid down, or any decisions made, on or after exit day by the European Court, and*
>
> *(b) cannot refer any matter to the European Court on or after exit day.*

(2)A court or tribunal need not have regard to anything done on or after exit day by the European Court, another EU entity or the EU but may do so if it considers it appropriate to do so."

[10] See eg https://www.infosecurity-magazine.com/news/uk-writes-gdpr-into-law-data and http://blogs.lse.ac.uk/mediapolicyproject/2016/12/19/could-the-european-gdpr-undermine-the-uk-investigatory-powers-act/

[11] See https://www.lawscot.org.uk/media/769016/080416-priv-call-for-evidence-on-the-investigatory-powers-bill-response-law-society-of-scotland-2-.pdf

[12] https://publications.parliament.uk/pa/bills/cbill/2017-2019/0005/cbill_2017-20190005_en_2.htm#pb2-l1g6

However, any decision of the CJEU relating to the GDPR will determine how it is interpreted in the EU and accordingly influence the parameters or adequacy of third countries. If the UK interpretation of the rules originating in the GDPR were to diverge significantly from that of the EU it could therefore jeopardise an adequacy decision.

Other international arrangements

Once the UK ceases to be a member of the EU, the Privacy Shield scheme for EU-US data transfers would cease to apply. Presumably, the UK will be free to enter into whatever arrangements for data transfers it likes with the US, but how would this sit with the Data Protection Bill incorporating the GDPR into domestic law post Brexit?

Citizens' rights

It will not be possible for the UK to replicate the GDPR's rights for EU citizens to bring actions for annulment of decisions of the EU data protection board before the CJEU (in accordance with Art 263 TFEU): even if the UK sought to adopt and follow Board decisions, UK citizens would not have standing to bring such an action. It is not clear how the UK Government intends to address this.

Importance to UK businesses making use of personal data processing

Data is increasingly important to businesses, for example in driving service or product provision or facilitating targeted advertising. Businesses may also work in partnership on particular projects or for particular purposes so data processing firms or service suppliers may wish to carry out functions which means that they would fall within the definition of joint data controllers under the GDPR, for example where the data transferred/shared may fall within GDPR definition of personal data which includes "identification numbers, or online identifiers". It is critical to the business to know how to contract with such suppliers who may processing/transferring outside the UK following Brexit. It is not therefor merely about knowing how the UK will designate "adequacy" of others.

Codes of conduct for particular sectors

A further question is whether the Government intends to encourage specific associations and other bodies to draw up codes of conduct, as specified in Art 40 of the GDPR. If so, to which associations and sectors might this apply? This may well be an important development for some highly regulated sectors where organisations operate in very similar ways and will find GDPR compliance challenging.