SLAUGHTER AND MAY/

May 2023

SPOT THE DIFFERENCE: THE DPDI (NO 2) BILL STARTS ITS LEGISLATIVE JOURNEY

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 127 (May 2023)

For businesses across the UK and beyond waiting to see what a UK GDPR 2.0 might look like, the journey towards revised data privacy laws in the UK has begun (again). The Data Protection and Digital Information (No. 2) Bill ("2023 Bill") was introduced in the House of Commons on 8 March 2023. This is the second version of a set of proposals to reform the UK GDPR. The first version of the Bill ("2022 Bill") was introduced to Parliament in July 2022, but was withdrawn after governmental changes.

One of the aims of the reform is to make data protection compliance more straightforward in the UK and to promote innovation whilst maintaining high standards of data protection. Announcing the 2023 Bill, the Secretary of State, Michelle Donelan, said the "new common-sense-led UK version of the EU's GDPR will reduce costs and burdens for British businesses and charities" and promises to "unlock £4.7 billion in savings for the UK economy over the next 10 years". Given that the changes put forward in the 2022 and 2023 Bills do not represent a complete overhaul of the UK's data protection framework, and for some organisations may in fact end up having limited practical impact, it remains to be seen whether Donelan will be proved right.

The 2023 Bill, as with the 2022 Bill, amends the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations 2003 (as amended). The vast majority of the content in the 2023 Bill remains the same as the previous version. This briefing focuses on the key data protection amendments, looking in particular at the key differences between the 2022 Bill and 2023 Bill, the areas where the 2023 Bill could have introduced more clarity and/or flexibility for businesses, and the next steps in the reform process.

Legitimate interests as a legal processing basis

The 2023 Bill retains the proposed "recognised legitimate interests" (which do not require a balancing exercise to be carried out), including non-commercial interests such as national security, emergencies, crime and democratic engagement. Additionally, it states that direct marketing, network security and intra-group transfers are types of processing for which controllers *could* rely on legitimate interests. The explanatory notes to the 2023 Bill make it clear that these examples are illustrative and non-exhaustive, and controllers must still carry out a balancing test to ensure that their interests do not outweigh the rights, freedoms, and interests of individuals. The amendments have been welcomed by some – for example, the Data and Marketing Association has stated that "greater clarity" is "offered on what constitutes a legitimate interest, which will encourage more businesses to use it as a lawful basis for data processing where appropriate." However, these examples are already stated as being legitimate interests in the existing UK GDPR Recitals 47, 48 and 49, so for many this change will likely have limited practical impact.

The recognised legitimate interests included in the 2022 Bill were criticised for being limited and of relatively little use to the commercial sector and this has not changed in the 2023 Bill. A more extensive whitelist relevant to commercial contexts – including for example processing for human resources functions and fraud detection - would have been helpful.

In the absence of a more extensive whitelist, a wider acknowledgment that certain examples of processing in a commercial context "could" fall within the legitimate interests ground would be welcome. This is especially true given the legitimate interests ground has been in the spotlight in the UK and EU courts recently (for example in the UK Experian case and the CJEU having been asked to rule on whether a purely commercial interest can be considered a legitimate interest). However, the updated explanatory notes to the 2023 Bill do at least state that any legitimate commercial processing activity can be considered a legitimate interest, provided the processing is necessary, and appropriate consideration is given to the potential impact of the processing on data subjects.

This should help bolster the arguments for continued use of legitimate interests as a legal basis for commercial processing activities in the UK.

Senior Responsible Individual

The UK GDPR requires organisations to appoint a DPO if they are a public authority or where its core activities consist of (i) systematic monitoring of data subjects on a large scale, or (ii) large scale processing of special category data. The 2022 Bill retains the public authority requirement, but in contrast to the UK GDPR, only requires a Senior Responsible Individual (SRI) where an organisation carries out high-risk processing. The change was intended to help businesses cut red tape, especially where processing is at the lower end of the risk spectrum, but would in fact require UK businesses to assess whether they meet the new criteria for an SRI and EU/UK businesses to determine how the DPO and SRI functions interrelate. The 2023 Bill has not introduced further changes, which is disappointing given that more clarity in this area of concern would be welcome.

In particular, the EU GDPR (and current UK GDPR) requires that DPOs act in an independent manner and their tasks and duties do not result in a conflict of interest. This means they are not allowed to hold positions that lead them to determine the purposes and means of the processing of personal data, otherwise there would be a conflict of interest. For organisations operating across the UK and EU, this may be at odds with the 2022 Bill's requirement that a SRI be 'part of' senior management (although the Bill does contemplate that in cases of conflict of interest, the SRI must secure that the relevant task is performed by another). It is also unclear whether external or outsourced DPOs would be allowed to 'rebadge' as SRIs. Finally, although it is helpful that the 2022 Bill allows for the SRI to delegate their tasks to another person (who must be provided with appropriate resources and cannot be dismissed or penalised for performing those tasks), it remains unclear how the protections around job security would work in practice. Further amendments or guidance in this area would be welcomed.

Data Subject Access Requests (DSARs)

The UK government's apparent intention in the 2022 Bill was to curtail problematic data subject access requests, such as when DSARs are used to obtain information in the context of actual or potential litigation to avoid the civil procedure disclosure rules. The resulting amendments were to replace the threshold for refusing to comply with a DSAR from "manifestly unfounded" requests to "vexatious or excessive" ones. The 2022 Bill included examples of vexatious requests, including requests intended to cause distress; that are not made in good faith, or that are an abuse of process. These examples seemed promising but were not explained sufficiently to fully achieve the above objective.

The 2023 Bill updates the explanatory notes to clarify that the request need only be vexatious or excessive (and not both). This is helpful to some extent but the 2023 Bill and the explanatory guidance could have gone further in providing guidance on how to determine data subjects' intentions and the meaning of "abuse of process," and whether requests that aim to circumvent disclosure rules during litigation amount to an abuse of process.

It would also have been helpful to businesses if the 2023 Bill:

- put positive obligations on the data subject to cooperate with the controller, including to narrow the scope of their request,
- introduced a limit on the amount of time required to be spent by a controller responding to a DSAR, akin to those in the Freedom of Information Act 2000, and
- introduced a fee to submit DSARs through third parties and DSAR portals.

Scientific research purposes

The 2022 Bill added a reference that scientific research would mean "any research that can reasonably be described as scientific". The 2023 Bill further clarifies that the definition of scientific research includes "research carried out as a commercial activity." This would align the law with current ICO guidance and market practice and so, whilst this change is to be welcomed, it is merely codifying the current position rather than a material change.

Likewise, whilst the 2023 Bill provides a list of illustrative and non-exhaustive types of scientific research (such as applied or fundamental research or innovative research into technological development), these currently sit in UK GDPR recital 159. Whilst this change brings them into the operative provisions which is helpful, it is not a change in practice. Overall, the changes in this area are therefore unlikely to significantly facilitate use of data for scientific research in practice.

International Transfers

The 2023 Bill clarifies that transfer mechanisms entered into before the 2023 Bill's reforms take effect will continue to be valid under the new UK GDPR regime. This means that organisations that put in place the appropriate safeguards to comply with the recent rules on international data transfers will not need to re-paper (again) these arrangements. These appropriate safeguards include the UK international data transfer

tools introduced post-Brexit, namely, the UK international data transfer agreement and the UK addendum to the SCCs. This is a helpful clarification, although in practice, for many businesses repapering the SCCs with the latest versions remains a significant ongoing compliance exercise.

Records of processing of personal data

The 2023 Bill introduces a slightly more significant change to the obligation on organisations to maintain records of processing of personal data. The obligation to carry out the records of processing would in future only apply if the controller or the processor carries out processing that is "likely to result in a high risk to the rights and freedoms of individuals". In comparison, the 2022 Bill exempted organisations from record keeping where fewer than 250 people were employed and there was no high-risk processing.

Removal of the limitation on an organisation's size might be helpful for organisations that do not undertake high-risk processing. However, organisations will still need to comply with other UK GDPR requirements, such as accountability, transparency, DSARs and international data transfers, all of which are likely to require a data mapping (and recording) exercise of some sort to understand where the personal data is held and who it is shared with. This may limit the impact of the change in the 2023 Bill in practice.

Profiling, automated decision-making (ADM) and powers granted to the SoS

The 2023 Bill corrects some confusing drafting in the 2022 Bill which arguably suggested that profiling, despite being a form of ADM, could be more widely caught by the restrictions on ADM than other types of ADM. Whilst helpful, this change is quite minor.

The 2023 Bill also provides for the Secretary of State (SoS) to issue regulations specifying whether or not there is 'meaningful human involvement' in particular processing cases. The terms 'meaningful human involvement' were introduced in the 2022 Bill (and are retained in the 2023 Bill) to reflect existing guidance on how organisations should determine whether a processing decision is based solely on ADM and therefore is potentially subject to restrictions.

The SoS has also been granted a number of other new powers, including:

- the power to set strategic priorities for the ICO and to require the ICO to respond in writing as to how it will address them (although the ICO is not legally obliged to comply with them);
- the power to amend the list of recognised legitimate interests referred to above; and
- the power to approve statutory codes of practice published by the ICO. Where the SoS does not approve, it needs to explain its reasons so the ICO can revise the code and re-submit. If and when a code is approved, the SoS will lay it before parliament under the standard negative procedure.

The introduction and extent of these powers has been criticised by industry bodies, and most recently by MPs during the second reading of the 2023 Bill on April 17 (with Darren Jones, Labour MP, referring to them as Henry VIII powers that reflect the "ongoing creep of powers being taken from Parliament and given to the Executive"). The Public Law Project has similarly argued that "key provisions of the UK GDPR are to be subsequently amended via statutory instrument, an inappropriate legislative process that affords much less scrutiny and debate, if debates are held at all".

Concerns have also been raised that the SoS's powers to veto ICO guidance may erode the ICO's independence, which could then potentially jeopardise the UK's adequacy decision from the EU. Introducing this additional layer of oversight to the publication of codes of practice could in addition create further uncertainty for businesses and delay the production of valuable guidance. However, the government has reassured critics that the aim of the changes is to make the ICO more transparent and accountable and will still involve parliamentary scrutiny. Whether or not the level of parliamentary security provided for is appropriate given the potential benefits of an agile and adaptable data privacy framework in the UK remains to be seen and we may therefore see further amendments in this area of the reform.

Next steps

The 2023 Bill received its second reading on April 17 and the House of Commons Public Bill Committee has announced a call for written evidence. To be certain to be taken into account, written evidence should be provided by the Committee's first sitting on 10 May 2023. The Committee can however receive evidence up until it concludes its considerations, which can be earlier than the formal deadline for its report of 13 June 2023.

Organisations should consider if they wish to make representations as part of the legislative process. We have heard mixed views from Government sources as to the likelihood that the 2023 Bill will be materially amended through the process given the significant amount of consultation to date. A Government spokesperson has suggested that they expect the 2023

Bill to receive Royal Assent within a year of its introduction to Parliament in March this year. There is therefore no immediate urgency for organisations to start to plan for its introduction, but we recommend organisations follow the developments and consider over the coming months whether they want, and are able, to change their internal processes and governance to reflect any of the flexibilities. Organisations operating across the UK and EU will likely need to assess whether the cost of separating the UK data to benefit from the new regime is worth the advantage to be gained from its potential flexibilities.

In addition, although organisations compliant with the UK regime will largely be compliant with the new regime, they will need to make some changes to comply with the 2023 Bill if enacted in this form. This includes deciding how to deal with the changes to the DPO role and putting in place a transparent process to facilitate data subject complaints.

If enacted in this form, the 2023 Bill will therefore bring more compulsory changes to the internal compliance arrangements of UK businesses, and time will tell whether the other potential benefits of the reforms outweigh yet more changes in this area.

CONTACT

REBECCA COUSIN
PARTNER
T: 020 7090 4738
E: Rebecca.Cousin@slaughterandmay.com

LUCIE VAN GILS
ASSOCIATE
T: 020 7090 3560
E: Lucie.vanGils@Slaughterandmay.com

HILAL TEMEL
ASSOCIATE
T: 020 7090 3524
E: Hilal.Temel@slaughterandmay.com