Client Alert: UK Data Protection Bill

Date : September 18, 2017

Last Thursday the UK Government published its new Data Protection Bill, currently known as the Data Protection Bill 2017. The Bill, when it becomes law, will become the third Data Protection Act in the UK.

The Bill largely follows the Government's Statement of Intent. You can find a summary of the Government's proposals and a short film here: www.bit.ly/ukgdpr.

The Bill is a big piece of work. It has 194 Sections and 18 Schedules. Altogether in its official draft version the Bill is 218 pages long. The basic intentions are to implement the GDPR regime, to preserve and improve some of the differences between the 1995 EU Data Protection Directive and the Data Protection Act 1998 (such as the introduction of the new criminal offences that we spoke about in our earlier alert), and to deal with the maintenance of GDPR in UK law should the UK leave the EU. The relationship between the new Bill and GDPR is a little complex. Since GDPR is a Regulation implementing legislation is not strictly necessary but the UK – in common with other EU countries including Germany, Hungary, Ireland and Portugal has decided to update its own data protection law at the same time.

The Bill still has some way to go before it becomes law. It is unlikely to pass without changes being made although the level of scrutiny it receives in Parliament remains to be seen with Brexit taking up much of Parliament's time.

We will be going through some aspects of the Bill in our next GDPR Navigator call. There are details of GDPR Navigator here: www.bit.ly/gdprnav. For now however, the following might be of interest:

Child's consent

As anticipated the UK intends to modify GDPR in UK law by lowering the age at which a child can consent from 16 to 13. This is permitted as a derogation from GDPR but the lack of uniformity across the EU may cause issues for some organisations.

Fees for dealing with data subject's rights

The general principle of GDPR is that data subjects get to exercise data subject rights (like subject access requests or SARs) free of charge. In some limited circumstances however organisations can make a charge. s.11 of the Bill allows the Government to introduce caps on those fees.

Accreditation of certification providers

We've talked a lot this year about GDPR fake news. You can see our blog and our film on that at www.bit.ly/gdprfake. We've seen a rise in unqualified bodies – often with little experience in data protection – claiming to be "GDPR certified" or "GDPR accredited". s.16 seems to be an attempt to deal with that making it clear that accreditation as a certification provider is only valid when carried out by the ICO or an approved national accreditation body. There is a procedure to be gone through before the ICO accredits a certification provider. For the avoidance of doubt nobody is certified yet in the UK.

Transfers of personal data

s.17 of the Bill seeks to embody the same system for data transfers as we outlined in our GDPR FAQs (see www.bit.ly/gdprfaq). More power is given to the UK Government. Data transfers are still likely to be a challenging topic in the coming months with the challenges to Privacy Shield and its review (see http://www.corderycompliance.com/privacy-shield-faqs/) and given the judgment in the Schrems III case dealing with Standard Contractual Clauses (http://www.corderycompliance.com/client-alert-schrems-irish-case-referred-to-european-court-threat-to-model-

clauses-and-international-data-transfers/). Data transfers could become yet more complicated in April 2019 if the UK withdraws from the EU. s.72(b) makes it clear that adequacy decisions can be repealed or suspended.

Records of processing activities

We've seen a lot of mis-statements regarding the obligations on data controllers to keep records under Article 30 of GDPR. The Article 30 provisions are essentially carried across into s.59 of the Bill. s.59(2) sets out the details that should be in a data controller's record to comply with s.59. In line with guidance from some data protection regulators this largely mirrors the current notification under the Data Protection Act 1998 (DPA 1998). s.59 does not require a complete log or data map of all personal data that an organisation holds. s.59 also has similar but separate provisions obliging data processors to keep their own records. These records must be made available to the ICO on request.

In addition, s.60 creates obligations on a data controller to keep logs dealing with some forms of automated processing. Again, these logs must be made available to the ICO on request.

DPIAs

From our experience of working with organisations, Data Protection Impact Assessment (DPIA) seems to be one of the most difficult areas of GDPR planning but also a process that, once mastered, brings significant benefits to the business. Our GDPR Navigator subscription service includes a number of tools to help with the DPIA process including a film explaining the process (see www.bit.ly/gdprnav). s.63 of the Bill explains how consultation with the ICO will work when the DPIA indicates that the intended processing would result in a high risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk). The DPIA has to be provided to the ICO together with any other information which the ICO asks for to make an assessment of compliance. Where the ICO feels that the DPIA would infringe the relevant part of data protection law, the ICO has to provide written advice to the data controller and, where the data controller is using a data processor, to the data processor as well. The ICO has six weeks to deliver its written advice beginning with receipt of the request for consultation. The ICO can extend this six week period by a further one month in complex situations. If the ICO does need an extension there is a process for the ICO to go through.

Income generation

There has been quite a bit of speculation about how the ICO would be funded, particularly if the ability to charge a fee to notify the Information Commissioner goes. We wrote earlier this year on the ICO's Annual Report (see http://www.corderycompliance.com/client-alert-uk-data-protection-regulators-report-shows-likely-gdpr-activity/). In the 2016/17 accounts the ICO showed an income from activities of just over £20m which included just over £19.7m in fees collected under the Data Protection Act 1998 for registrations. One of the commitments made when GDPR was going through the legislative process would be that red tape would be reduced for businesses and there has long been an assumption that registration fees would go. s.129 opens the door however for the ICO to charge "a reasonable fee". There is a similar power to levy charges in s.132 of the Bill. We do not yet know what this might be and again, there is a process described in the Act for introducing fees and charges but it could be the case that consultation with the ICO for a DPIA might be a way of filling the revenue gap for the ICO. At this stage however, this is just speculation.

Fines

The system of monetary penalties under the current DPA 1998 goes and is replaced with a new system of penalty notices under s.148. In many respects the regime stays the same but with the much talked about higher levels of fines available to match GDPR. s.148(3) is likely to be helpful to any organisation that discovers a breach as it lists some of the factors that the ICO will take into account in setting the penalty. Again, much of this is not new and the list certainly reflects the ICO's enforcement activity in recent years but the section makes it clear that the setting of fines will continue to be an area where a number of factors come into play. You should remember that fines are not the only game in town however, and the Bill also reflects other provisions of GDPR including the power to require

the suspension of data processing operations.

Despite some of the talk of possible interest rate variations since the Government trailed the maximum fine at £18m, fines do actually track to GDPR with a mechanism in s.150(7) to use the Bank of England exchange rate to ensure that the level of fine tracks to the Euro amount specified in GDPR.

s.152 gives the Government the power to add in some of the fine detail about fines such as specifying what an undertaking is, what a financial year is and how turnover is to be determined in assessing a fine. Before making these changes "*the Secretary of State must consult such persons as the Secretary of State considers appropriate*". Anyone concerned about how the fining regime may work might want to consider making representations to the Secretary of State accordingly and asking to be part of that consultation process.

Complaints by data subjects

GDPR gives data protection regulators greater powers but also, in some circumstances, they are subject to greater accountability as well. s.156 of the Bill sets out a process by which data subjects can complain to the ICO. If the ICO fails to act on the complaint then a data subject can complain to a special tribunal who can order the ICO to take appropriate steps or give the data subject a progress report. As a general rule a complaint to a tribunal can be made if the ICO fails to take action or fails to report on progress within three months of receipt of the complaint. In addition to the rights to complain to a tribunal, s.158 also gives data subjects the right to complain to a court if their data subject rights have been contravened. Another aspect of GDPR fake news that we've commented on before (see www.bit.ly/gdprfake) is that the new rights won't be enforced. As we've said before we do not think that that is the case and the fact that data subjects also have the right to involve a tribunal or the courts is likely to mean that action could be taken against a company even if the ICO refuses to investigate. In addition, the much talked about right to compensation in GDPR is included in the Bill in s.159 and s.160.

Unlawful obtaining of personal data

In our earlier alert we talked about the Government's intention to introduce new criminal offences. s.161 is the extension of an existing offence of unlawfully obtaining personal data. The difference between s.161 and the current s.55 DPA 1998 is principally a new offence of retaining personal data without the consent of the data controller when the data was obtained. This will apply potentially if data was given to an organisation by a data controller and wasn't returned when the data controller asked for it back.

Re-identification of de-identified personal data

As we've said in our earlier alert, the Bill includes a new offence in s.162 of knowingly or recklessly re-identifying information that is de-identified personal data without the consent of the data controller. This section intends to criminalise the identification of a data subject from anonymised or pseudonomysed data. It might be particularly worrying for example in the online marketing context where sometimes statistics on web use or click rates are provided on a pseudonomysed basis but the recipient of the data can work out individual behaviours from data it has in its possession. There are some defences available to the offence but care will need to be taken and the risks in re-identification will need to be built into training.

Destroying data subject to a SAR

There is also a new offence in s.163 of altering personal data to prevent disclosure. This offence can be committed when a SAR has been made and the person making the request would be entitled to receive information in response to the request but the data has been altered, defaced, blocked, erased, destroyed or concealed with the intention of preventing disclosure. The data controller can be guilty of this offence as can any person who is employed by the controller, an officer of the controller, or anyone who is "*subject to the direction of the controller*". Again, there are some defences available but organisations will need to make sure that they alter their SAR response processes to make sure that criminal offences are not committed and they will also need to adapt their training to emphasise the importance of dealing properly with SARs.

Employment and health records

We talked before about the criminal offence of requiring the production of employment records (see www.bit.ly/icohr). Broadly those provisions continue in s.171 of the Bill, s.172 looks at contracts that require individuals to supply another person (such as their employer) with information in a health record. Any terms and conditions (for example terms and conditions of employment) which require that are likely to be void under s.172. This, coupled with the greater difficulties in obtaining consent, is likely to mean that organisations are going to have to take a thorough look at their hiring practices where they currently require health data, including tests for substance abuse.

Personal liability of directors, managers etc.

In common with the existing legislation, the so-called consent and connivance provisions, s.177 preserves the ability of prosecutions to be brought against individuals. This includes directors, managers, secretaries or similar officers. It could also apply to members of a LLP and partners in a partnership.

What should you do now?

Most organisations will be well on their way with their GDPR preparation. If the UK is an important market they would be wise to make sure that their GDPR plan takes into account the differences that the Data Protection Bill will provide. It might not be certain what the new legislation will look like, but it will be possible to take an educated guess. As part of your compliance with the new legislation, and GDPR generally, you should consider the following:-

1. Put in place a DPIA process – make sure risks are identified and reduced (or better still eliminated!);
2. Thoroughly review vendor contracts – you will need your vendors' help especially in reporting security breaches very quickly. Make sure that you have the contractual rights to insist on this and make sure that you can hold your vendors to account;
3. Prepare to update everything and prepare new detailed documentation and records ready for production for regulatory inspection – factor this into overhead costs;
4. Review how you collect data, what you use it for, who has access, how long you keep it for and how you'll get rid of it;
5. Ensure that new aspects such as explicit consent, the right to be forgotten, and, the right to not be subject to profiling are all included in policies and procedures. An SAR process is especially important given the new criminal offence;
6. Put in place a data breach notification procedure, including detection and response capabilities – make sure you secure hard copies as well as electronic data;
7. Train staff on all of the above;
8. Set up and undertake regular compliance audits in order to identify and rectify issues; and
9. Stay informed – the requirements are changing and you'll need to keep on top.

This alert first appeared on 18 September 2017 and has been updated to reflect the Schrems judgment.

Details of Cordery's data protection and privacy practice are at http://www.corderycompliance.com/data-protection-privacy/ and details of our training solutions are at http://www.corderycompliance.com/solutis/training/.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com