Client Alert: Data Protection Act 2018

Date : May 24, 2018

The UK's new data protection law, the Data Protection Act 2018 (DPA 2018), received the Royal Assent yesterday. This is the third Data Protection Act in the UK and is an important part of the UK's implementation of a new data protection regime alongside the General Data Protection Regulation (GDPR) which comes in tomorrow. DPA 2018 and its various appendices come in at 339 pages in the official version. You can find out more about the history to DPA 2018 in our alert and film here: http://www.corderycompliance.com/client-alert-uk-data-protection-bill/.

What does it say?

In many respects there are no surprises. DPA 2018 builds on the data protection foundations of previous UK law, the Data Protection Act 1998 (DPA 1998), but with changes to reflect changed circumstances and also to match the GDPR regime.

When will it come into force?

Most of the provisions of DPA 2018 come into force tomorrow i.e. 25 May 2018. Some of the other provisions that will not have as much impact on businesses come in on 23 July 2018.

New criminal offences

We've talked in our film previously about new criminal offences created by DPA 2018. These new offences include:

- s.170 – an extended offence of unlawfully obtaining data or refusing to return it when the data controller asks for it back;
- s.171 – a new offence of re-identifying anonymised or pseudonymised data;
- s.173 – a new offence of altering data to prevent disclosure to a data subject after a data subject makes a request under GDPR or DPA 2018.

There are various defences in DPA 2018 to these new offences. One of the defences to a s.173 prosecution could be that the *"alteration, defacing, blocking, erasure, destruction or concealment"* of the information would have occurred even if a data subject request had not been made. This should mean that in some circumstances routine data housekeeping would not attract a criminal penalty, although organisations will want to put measures in place to ensure that they comply with the law when receiving a valid request. A charge under s.173 would be heard by a Magistrates Court in England and Wales, but a charge under s.170 or s.171 could also be heard by a Crown Court. On a conviction under s.170 the court could order documents to be confiscated.

There is more information on Subject Access Requests more generally in Jonathan Armstrong's podcast with Tom Fox here: http://www.corderycompliance.com/countdown-to-gdpr-episode-8-subject-access-requests/. Cordery's GDPR Navigator includes detailed guidance on data subject rights and how to handle them.

There are some additional offences in DPA 2018 notably around obstructing or misleading the ICO. Schedule 15 of DPA 2018 gives the ICO extended powers of entry and inspection. It is an offence for any person to intentionally obstruct the ICO in exercising their new powers, or to fail to provide any assistance that the ICO requires. Making false statements to the ICO can also be prosecuted – this means that statements following a data breach for example will require more careful consideration.

In addition, a new offence is created in s.148 of destroying or falsifying information and documents if an information notice or assessment notice has been served by the ICO. As with the other offences that we have mentioned various defences do exist.

s.184 of DPA 2018 creates two criminal offences which can be committed, for example, if an employer requires an employee to provide specific records as a condition of their employment or continued employment. This offence basically follows the enforced access request prohibition which came into UK law in March 2015 and which we wrote about here: http://www.corderycompliance.com/enforced-access-request-prohibition-comes-into-force-on-10-march-2015/. There are some additional offences which are not likely to affect the majority of our clients.

Personal liability of directors, managers etc.

In common with the predecessor DPA 1998, DPA 2018 contains so called "*consent and connivance provisions*". This means that under s.198 of DPA 2018 "*a director, manager, secretary or similar officer*" of an organisation or anyone who purported to act in that capacity can also be convicted of a criminal offence if the organisation commits the offence and the relevant individual consented, connived or neglected in taking their responsibilities seriously and contributed as a result to the offence being committed. Offences under s.170, s.171 and s.173 as highlighted above also become recordable offences – that is to say an organisation or an individual committing an offence would have a criminal record on conviction.

Enforcement notices

Where a data controller or a data processor (or some other types of body such as a certification provider) has failed or is failing to comply with their obligations under DPA 2018 and/or GDPR, the ICO can issue them with a written enforcement notice requiring them to either take and/or refrain from taking some specific steps. It is likely that the ICO will use enforcement notices in a large number of cases just as they have under the prior DPA 1998 regime. Enforcement notices can ban data controllers and data processors from processing all or some personal data; order them to rectify or erase personal data which they hold; and/or notify third parties who they have disclosed personal data to. In some cases an enforcement notice could have more severe consequences than a fine – for example if an enforcement notice prohibited a company from maintaining its whistleblowing helpline that could trigger a report to a stock exchange or a failure to meet mandatory corporate governance requirements.

Penalty notices

If an organisation fails to comply with an enforcement notice, an information notice or an assessment notice the ICO can issue a written penalty notice imposing a fine on the recipient. There are various factors the ICO would take into account when setting a fine which are outlined in our guidance in GDPR Navigator. The maximum level of fine that can be imposed via a penalty notice varies on the nature of the breach, but fines of up to €20m or 4% of worldwide annual turnover are possible – that is the same level as in GDPR. The maximum amount of the penalty in sterling is determined by applying the spot exchange rate set by the Bank of England on the day on which the penalty notice is given.

Do I still need register with the ICO?

Probably. One of the promised benefits of GDPR was the removal of data protection registration requirements across the EU. The UK however retains the obligation to register with the Information Commissioner's Office (ICO) despite GDPR. The new regime is outlined in a separate piece of legislation, the Data Protection (Charges and Information) Regulations 2018, which require a data controller (unless exempt) to deliver information to the ICO on their staff, turnover etc. so that the registration fee can be assessed. The new registration regime will be in place tomorrow. It will be in many respects similar to the DPA 1998 regime, but in some cases with increased notification fees. The fees range from £40 to £2,900 per annum.

You can find out more about the history to DPA 2018 in our alert and film here: http://www.corderycompliance.com/client-alert-uk-data-protection-bill/. You can find out more about GDPR in our GDPR FAQs here: http://www.bit.ly/gdprfaqs and with our GDPR Navigator subscription service, the details of which are here: http://www.bit.ly/gdprnav.

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