The Data Protection Bill: A Summary

By Lynn Wyeth

The text of the new Data Protection Bill has finally been published by the Government and at 218 pages, 194 clauses, 18 schedules and 112 pages of explanatory notes, it is a huge chunk of legalese spaghetti. You can find the main Bill in pdf form here.

As with the 1998 Data Protection Act (DPA98), the Bill is cumbersome and repeatedly refers to clauses within itself. This is compounded this time by references also to the General Data Protection Regulation (GDPR) and other pieces of European legislation. To translate all this and join all the dots you need to flick between many texts and screens, but here's a quick summary of some of the key issues and where to find them in the Bill:

Structure of the Bill

There's nothing hugely unexpected in the Bill, as long as you are familiar with the DPA98, additional orders added to the DPA98 over the years, the GPDR and the Law Enforcement Directive (EU) 2016/680! This has all been merged into one large Bill to try and keep what we have now plus any new requirements of GDPR and the Directive. The Bill is set out in Parts, some of which may not be relevant to all organisations.

Part 1 & 2 – Definitions and General Processing
Part 3 – Law Enforcement
Part 4 - Intelligence Services
Part 5 – Information Commissioner's Office
Part 6 - Enforcement
Part 7 – Miscellaneous!

Law Enforcement

Part 3 of the Bill deals exclusively with Law Enforcement under Clauses 27 -79. Organisations will only be subject to these clauses if they are

- a Competent Authority, or
- processing for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Schedule 7 lists the Competent Authorities and this includes organisations such as Government departments, Police, Fraud Office, Probation, Youth Offending Teams etc. If you don't meet the criteria above, you don't need to worry about this large part of the Bill.

There are some differences in Part 3 that organisations do need to be aware of if they fall into the law enforcement category. The Data Protection Officer (DPO) has extra specified tasks in clause 69, namely the ability to assign responsibilities, promote policies, undertake audits and deliver training. There is also an additional requirement to have specific audit

trails (clause 60 - logging) on automated processing ensuring a log of who collected, altered, erased and transferred data amongst other things.

Public Authorities

The Bill confirms in clause 6 that where it refers to public authorities or public bodies, it means those organisations that are currently subject to Freedom of Information Act provisions. Interestingly it means any organisations brought under FOI in the future may need to consider issues such as DPOs and use of legitimate interests in future too. Housing associations and companies delivering public contracts may need to watch the FoI Private Member's Bill going through parliament next year or the ICO's push for extending FOI through its reports to Parliament.

Data Protection Officers

For those organisations not involved in law enforcement, their DPO will only have to undertake the tasks set out in GDPR, not the additional ones set out in clause 69. There are no extra surprises here and the Article 29 Working Party guidance on this is comprehensive about when one is required by law, the tasks it carries out and on the issue of conflict of interest. Senior managers, SIROs, Caldicott Guardians, Heads of IT or HR… none of them can be the DPO.

Data Breaches

As expected in order to implement the GDPR requirements, any personal data breaches must be reported to the Information Commissioner's Office (ICO), where there is a risk to an individual, within 72 hours unless there is reasoned justification (breach notification). The potential derogation for public authorities has not been taken advantage of and they, like all other organisations, could face Civil Monetary Penalties (CMPs) of up to £17m or 4% of the equivalent of annual global turnover (although the ICO can change this – perhaps due to currency fluctuation or after Brexit). The reality is that the ICO, as stated in its myth busting blog, will continue to use CMPs as a last resort and they will be proportionate.

Children

The Bill also confirms that in the UK the child's age in relation to *information society services* will apply if the child is under 13 years old rather than 16 years old. Providers of such services will have to take reasonable steps to get the consent of a parent or guardian to offer a child under 13 years the service. The definition of *information society services* can be found in the E-Commerce Directive and it should be noted this specific age of consent is only for this type of service. For all other data protection issues, children can make their own decisions if they have capacity or *Gillick competency*. Data Protection practitioners in Scotland have the added complexity in clause 187 of separate rules for age of consent for Scottish children to reflect the existing provision there now that *"a person aged 12 or over is to be presumed to be of sufficient age and maturity to have such understanding, unless the contrary is shown".*

Fees

As previously discussed on this blog, GDPR removes the obligation for data controllers to notify with the ICO. The ICO had expressed concerns about this and the loss of income if they could not continue with notification fees (currently £500 per annum for large organisations, £35 per annum for smaller data controllers). The Data Protection Bill therefore makes provision for the ICO to continue to require a form of notification fees under clause 129. In fact, the Bill looks like it allows the ICO to charge fees for other services too. The ICO will have to publish these fees and have them agreed by the Secretary of State. The DCMS is currently consulting on a 3-tier system with the top tier (businesses with over 250 staff) having to pay up to £1000 (with a direct marketing top up of £20).

Conditions for processing

The ICO has already stressed in its myth busting blog that consent is not the only condition for processing despite misleading stories elsewhere. As before, the Bill lists several conditions for processing non-sensitive personal data and sensitive (now called special category in GDPR) personal data. As we already knew from GDPR, Public Authorities can no longer rely on legitimate interests but all of the other conditions from the existing DPA98 have been brought across e.g. counselling, insurance**.** There's even one explicitly for anti-doping in sport. Schedule 1 lists all of these conditions for processing special category data.

Complaints and compensation

Clause 157 sets out what individuals can expect if they submit a complaint to the ICO and the ICO fails to address it adequately, and how the Tribunal can then become involved. Clause 159 provides for compensation claims for 'damage' and that can include financial loss, distress and other adverse effects. Consumer support groups are disappointed that they are not able take class actions and seek redress without the data subject's consent, as the Government has decided against the use of that derogation.

New Criminal Offences

There will be a new criminal offence under the Bill where anyone uses anonymised data "knowingly or recklessly to re-identify information that is de-identified personal data". Researchers and IT testers will need to be careful that they can demonstrate anything accidently re-identified or deliberately tested is done in the public interest and doesn't trigger this offence. Data theft will also be a recordable offence on the national police computer, as will unlawfully obtaining personal data and altering personal data in a way to prevent it being disclosed.

Certification

Clause 16 allows for the accreditation of certification providers. The only organisations that can award certification are the ICO and the National Accreditation Body (which looks set to be UKAS). No organisation has been awarded certification yet so beware of organisations claiming they can make you a 'certified' GDPR practitioner at this time!

Exemptions
All of the familiar exemptions have been brought across from the current DPA98 e.g. crime and taxation, journalism, references, examination marks, honours, parliamentary privilege, management forecasts, legal professional privilege and negotiations. Also added is immigration, and clarity is given on archiving and research. They can all be found in Schedules 2-4, with Schedule 3 focussing on detail on health and social care, and schedule 4 on education, child abuse and adoption.

Subject Access Requests
The Bill confirms the requirements in the GDPR. You cannot charge for a Subject Access Request unless repeated or manifestly unfounded or excessive, and you must answer in one month (unless it's excessive and it can be extended for another two months).

What happens next?
The 2nd reading of the Bill will take place in the House of Lords on October 10th 2017. Its passage through Parliament can be tracked here. There may be some amendments made as it works its way through the parliamentary process. Several Regulations will also need to be made by the Secretary of State to implement some parts of the Bill, and Act Now will bring you any updates as they happen.

Lynn Wyeth is the Head of the Information Governance function of a large unitary public authority and has over 10 years' experience as a Data Protection and FOI practitioner. She also delivers some of our external GDPR and GDPR Practitioner Certificate courses.