

# Expert comment

**Rob Corbet is a  
Partner at Arthur  
Cox and Member  
of the Examination  
Board for the  
Practitioner  
Certificate in Data  
Protection — the  
views expressed  
are his own**

**O**n 1st February 2018, the Data Protection Bill 2018 was finally published. With just 114 days to go before the GDPR commences, adoption of the Bill will require a fast-track attention of the Oireachtas if it is to make it through various legislative stages (i.e. debate stage, committee stage, report stage and signature by the President) in time.

Unsurprisingly, the Bill, which runs to 162 Sections and 3 Schedules, does not deviate in many respects from the principles set out in the General Scheme of the Bill which was published in summer 2017. Whilst the specific measures in the Bill will be explored in depth in future editions, below are some immediate impressions on the draft Bill.

## How the Bill fits in with GDPR

The Bill has been drafted to transpose both the GDPR and Directive 2016/680/EC which deals with data protection in law enforcement matters (Part 5 of the Bill). However, happily the Data Protection Acts 1988 and 2003 will be replaced by the Bill, save in limited circumstances dealing with national security, defence and international relations. The practical impact of this is that Parts 1 – 4 and Parts 6 – 7 of the Bill will need to be read in conjunction with the GDPR in order for practitioners to have a complete understanding of Ireland's data protection laws after 25th May 2018.

The Bill also provides for Ministers to adopt secondary legislation in various areas, for example in further defining public interest processing (Section 45) or in the area of restricting data subject rights for general public interest purposes (Section 54(6)).

## Powers of the ODPC

Part 6 of the Bill deals with the extended powers of the ODPC. In contrast with the current unsatisfactory position whereby the ODPC is mandated to investigate every complaint unless 'frivolous or vexatious', Section 91 of the Bill permits the ODPC to refuse to act on a request (or to charge a fee) if it is manifestly unfounded or excessive. While that may seem like splitting hairs, Sections 103 and 104 appear to provide the ODPC with a broader discretion to reject or dismiss a

complaint or to take such action as the ODPC considers appropriate. The only obligation seems to be to report to the data subject on the progress or outcome of the complaint within 3 months. While generally decisions of the ODPC will be subject to judicial review, it appears from Section 145 (12) (although it is not entirely clear) that the ODPC has the final decision as to whether to reject or dismiss a complaint.

Section 122 lists a range of 'coercive powers' that may be imposed by the ODPC (separate to Information and Enforcement Notices), perhaps suggesting that administrative fines should be viewed as a last resort. In addition, Section 130 of the Bill gives the ODPC a new power to compel the production of an expert report commissioned by the controller/processor and at its own expense on any specified GDPR-related matter. As was the case in the General Scheme of the Bill, Section 138 applies a Court validation process to fines imposed by the ODPC, even in circumstances where the controller has not appealed the fine.

The myriad of powers afforded to the ODPC under the GDPR and the Bill and the associated procedures to be followed in each case are complex. One could imagine many situations where a single complaint could lead to multiple different actions on the part of the ODPC, the complainant and the controller or processor affected, one or more of which could result in an appeal or judicial review.

## No class actions for damages

As expected, Ireland has availed of the option not to permit non-profit bodies to bring class actions for damages (Section 123(7)), although such bodies can bring actions for various other remedies and reliefs.

## Limitations on data subjects' rights

Article 23 GDPR allows Member States certain discretion to restrict the scope of data subject rights (including the rights of access, erasure, rectification and portability). Sections 54 and 55 of the Bill set out Ireland's proposed approach in this regard. As Section 54 impacts on all controllers regardless of their public/private sector status

or the industries involved, it will have significant impact and will be carefully scrutinised. Many of the restrictions reflect those in Section 5 of the existing Data Protection Acts but there are some interesting changes, including in the case of the enforcement of civil law claims, liabilities and debts. Section 54 also provides for future regulations introducing more specific restrictions.

## Digital age of consent set at 13

Section 29 of the Bill confirms that Ireland's so called 'digital age of consent' is set at the minimum age of 13 permitted by Article 8 GDPR. Some media reporting on this issue has been misleading, as it fails to reflect the very narrow circumstances in which this provision is relevant. Article 8 is only engaged when a controller is providing online services to children and is relying on consent as the lawful basis to do so. Where the controller is relying on alternative lawful bases for providing the online service (such as legitimate interests or contractual necessity), Section 29 does not apply. Section 29(2) also confirms that the requirement to obtain parental/guardian consent for children under 13 does not apply to preventative or counselling services.

## Brexit proofing

The Bill includes an interesting provision in Section 34 which seems intent on preserving the free movement of data between the UK and Ireland in the context of the common travel policy. This is a clever provision, no doubt intended to bring some legislative clarity to cross border free movement issues between Ireland, Northern Ireland and Britain regardless of what specific measures accompany Brexit.

## Fines — good news for public bodies?

Section 136(3) of the Bill appears to try to exempt public bodies from the fines regime under the GDPR. However, this issue is not beyond doubt. The section is currently ambiguously worded and would benefit from

greater clarity as the Bill progresses. Currently, the section provides that the ODPC 'may not decide to impose an administrative fine on a controller or processor that is a public authority or body only where the authority or body acts as an undertaking within the meaning of the Competition Act 2002'. While the intent seems to be to include public bodies in the fines regime where they are competing with private sector bodies, it is not clear that public bodies are otherwise exempt from fines.

## 'Suitable and specific measures'

The term 'suitable and specific measures' is a new term which is likely to quickly enter into the popular lexicon of Irish data protection practitioners. This is because Section 40 of the Bill defines a series of measures which 'may' constitute 'suitable and specific measures' which can be adopted by controllers and processors in certain circumstances. The measures themselves are something of a mixed bag, ranging from 'explicit consent' (which seems to confuse 'measures' with fundamental legal bases) through to training, access limitation within workplaces, data logging, pseudonymisation, and encryption.

This seems to be an attempt to provide some legislative support for controllers/processors adopting a risk-based approach as permitted by Article 24 GDPR, while also providing a framework for any future ministerial regulations of the type referred to above. For example, Section 40 of the Bill permits employers to adopt suitable and specific measures in the context of supporting the processing of special categories of data (health, etc.) in the workplace, Section 44 includes similar accommodating provisions for the insurance, pensions and mortgage industries while Sections 46 and 47 address the health sector. Section 49 introduces some similar criteria in the context of convictions data which would otherwise be unlawful under Article 10 GDPR. Again this measure will be welcomed by the financial services industry in the context of fraud prevention.

## Respecting the essence of data protection

Similar to 'suitable and specific measures', another interesting feature of the Bill is the facilitation of certain processing activities if they 'respect the essence of data protection'. It is unclear what this phrase means but it could have wide implications. For example, processing of special categories of personal data pursuant to an enactment is required by Section 43 to be subject to both 'suitable and specific measures' while also respecting the essence of data protection.

## Conclusion

The Data Protection Act 1988 lasted 30 years and was only materially amended once (in 2003). The Data Protection Bill 2018 could easily have a similar lifespan and as such, from a regulatory perspective, it is a shame that there is so little time available to consider its implications and adopt improvements.

Also and on a practical level, there is simply insufficient time for most controllers and processors to digest the contents of the Bill when they are already struggling with all of the complexity and ambiguity presented by the GDPR itself. Hopefully the above short summary will be of some assistance to those controllers and processors who will be subject to Irish jurisdiction under the GDPR.

---

**Rob Corbet**

Partner

Arthur Cox

rob.corbet@arthurcox.com

---