A&L Goodbody

Irish Government Publishes Data Protection Bill 2018

The Government has published the eagerly awaited Data Protection Bill 2018. The Bill incorporates Ireland's national implementing measures required under the GDPR and creates a new regulatory framework for the enforcement of data protection laws in Ireland.

Top ten highlights

Highlights of the Bill include:

1. Confirmation that 13 years will be the "digital age of consent".
2. Provisions enabling non-profit bodies to represent data subjects in complaints to the Data Protection Commission (**DPC**) and in bringing data protection claims before the courts.
3. Abolition of the requirement for data controllers and processors to register with the DPC.
4. The exemption of most public bodies from administrative fines.
5. An apparent Brexit proofing provision that will allow airlines and ships to transfer personal data for the purpose of preserving the Common Travel Area between the UK and Ireland.
6. Derogations for freedom of expression, processing of health data for insurance/pension purposes, and processing of criminal convictions data.
7. Enabling provisions for when the DPC acts as the lead supervisory authority under the "one-stop-shop" regime.
8. New investigative powers and procedures for the DPC. These will include expanded powers to gain access to electronic records, provision for the drawing up of investigative reports, the appointment of expert reviewers, and the conduct of oral hearings.
9. Conferring of jurisdiction on the High Court for some appeals from the DPC and in data protection claims over a certain threshold.
10. Confirmation that the Data Protection Act 1988 will be repealed for data processing generally, but retained insofar as it will still apply to processing of personal data for purposes of national security, defence and international relations of the State.

In Depth

What is the reason for the Bill?

From a practical perspective the Bill is as important as the GDPR itself. Whereas the GDPR contains the substantive directly effective principles of EU data protection law, the Bill establishes the administrative and enforcement machinery necessary to give effect to those principles. With the introduction of an administrative fines regime and the possibility of recovering 'immaterial' damage for data breaches, these aspects of the Bill will be of real significance to all businesses that process personal data.

The GDPR is due to come into force on 25 May 2018. For the Bill to pass through all stages of the Oireachtas in less than 4 months, with the necessary enabling regulations and administrative arrangements in place, will be very challenging. Other EU states are also struggling to meet the deadline - to date only Germany and Austria have passed their GDPR enabling laws. It is to be hoped that the Government will give priority to the Bill so that Ireland can remain at the forefront of countries promoting effective and robust data protection regulation.

The Bill contains 162 sections and runs to 128 pages in length. It is a detailed and complex piece of draft legislation, which covers the following main areas:

(1) National implementing legislation for derogations and enabling provisions as permitted by the GDPR (Part 3).

(2) The re-establishment of the Office of the Data Protection Commissioner as the Data Protection Commission with provision for the appointment of up to three individual Commissioners (Part 2).

(3) Implementation of the Law Enforcement Directive, which is a parallel regime for data protection law applicable to any public authority with competence for investigating and prosecuting crimes (Part 5).

(4) The investigative and enforcement powers of the DPC, the enforcement procedure, the availability of judicial redress and details of criminal offences (Part 6).

In this update we draw attention to items 1 and 4 as these are of most relevance to businesses that are in the process of preparing for the GDPR and considering its future regulatory impact.

GDPR Derogations

Ireland is proposing to take a generally expansive approach to derogations permitted under the GDPR. Of particular note are:

Digital age of consent – The "digital age of consent" is the term used to refer to the requirement that consent to the processing of personal data by a child under the age of 16 years be authorised by that child's parent or guardian (to the extent that consent is being relied on where information society services are directly offered to a child). Ireland is opting to lower the age of consent to 13 years as permitted by Article 8(1) of the GDPR. This decision has been made following an extensive consultation process by the Government last year (Section 29(1)).

Lawful processing on public interest grounds – The GDPR permits processing that is necessary for the performance of a task carried out in the public interest or in the official authority vested in the controller. The Bill confirms that this includes a function conferred on a controller by an enactment or the Constitution, or for the administration of any non-statutory scheme, programme or funds (Section 34(1)).

Brexit derogation – An unexpected proposal is one that allows controllers that are airlines and ships to disclose personal data "*for the purpose of preserving the Common Travel Area*". The explanatory memorandum does not give the rationale for this derogation, but it would appear to be addressing the risk of potential interruptions to air and sea travel between the Ireland and the UK in the event that the UK leaves the EU without an agreement on the continued free flow of data being reached (Section 34(2)).

Further processing – The Bill provides for the processing of personal data for certain purposes other than the purpose for which it was collected. These include processing that is necessary for the purposes of preventing a threat to national

security and defence, or public security, preventing, investigating or prosecuting criminal offences, and for the purposes of providing legal advice and legal proceedings. This would include, for example, processing which is necessary for anti-money laundering purposes (Section 35).

Processing for archiving, scientific or historical research purposes or statistical purposes – The Bill confirms that personal data may be processed for these purposes, subject to such processing respecting the principle of data minimisation, and where identification of data subjects is no longer required, the processing should be carried out in a manner which does not permit such identification (Section 36).

Data processing and freedom of expression – The GDPR requires Member States by law to reconcile an individual's right to data protection with the right to freedom of expression and information (including processing for journalistic purposes, or for the purposes of academic, artistic or literary expression). The Bill provides that processing carried out for the purpose of exercising the right to freedom of expression and information shall be exempt from specified provisions of the GDPR, insofar as compliance with those provisions would be incompatible with such purposes. The Bill provides that in the right to freedom of expression shall be interpreted in a broad manner (Section 37).

Processing of special categories of personal data – Article 9 of the GDPR gives Member States some discretion in relation to the lawful bases to legitimise the processing of special categories of data (e.g. health, race or ethnic origin, trade union membership, political, religious or philosophical beliefs). In exercising this discretion, the Bill permits special categories of data to be processed where necessary for the purposes of providing legal advice, in connection with legal proceedings, or otherwise necessary for the purpose of establishing, exercising or defending legal rights (Section 41); and for the administration of justice and performance of a function conferred by an enactment or by the Constitution (Section 43).

Processing of health data for insurance and pension purposes - The Bill provides for health data to be processed where necessary for policies of insurance, life assurance, health assurance, pensions and the mortgaging of property. This derogation is intended to address concerns raised by insurance and pension providers at the pre-legislative stages (Section 44).

Processing of personal data relating to criminal convictions and offences – The GDPR permits criminal convictions and offences data to be processed only under the control of official authority or for specified purposes under national law. The Bill provides examples of processing under official authority (e.g. the administration of justice) and specifies five purposes where processing is permitted (Section 49).

Restrictions on individuals' rights - The GDPR permits Member States to make provision for restrictions on the exercise of data subjects' rights in certain circumstances. Section 54 of the Bill is particularly important. It replaces the restrictions currently set out in section 5 of the Data Protection Act 1988.

Imposition of fines on public authorities – The GDPR gives Member States discretion whether, and to what extent, administrative fines may be imposed on public bodies. The Bill provides that administrative fines may be imposed on a controller or processor that is a public authority only where it is acting as an "undertaking" within the meaning of the Competition Act 2002 (Section 136).

New Regulatory Framework

The Government has decided to overhaul the existing regulatory framework for enforcement of data protection law. Of particular note are the following:

Three forms of investigation – The Bill provides that there are three scenarios where an inquiry may be conducted by the DPC:

- By way of an investigation in response to a complaint that is received by either a data subject or a not-for-profit body established to represent data subjects;
- Where the DPC "of its own volition" causes an investigation into a suspected infringement of data protection law; and
- Where the DPC decides to conduct a "data protection audit" in exercise of its powers under Article 58(1)(b) of the GDPR.

The boundaries between a "data protection audit" and an investigation into a suspected infringement

by the DPC are not clear, and would benefit from further elaboration in the Bill.

Amicable resolution procedure - Similar to the procedure under the existing Data Protection Acts, the Bill provides for an amicable resolution procedure for complaints (Section 104(2)). Where the DPC believes that there is a "reasonable likelihood" of achieving an amicable resolution of a complaint, the DPC will attempt to facilitate such resolution. This is a welcome development, as it avoids a situation whereby the DPC would be obliged to make a formal decision on every complaint received, even where the complaint is easily resolved. The Bill also empowers the DPC to provide a complainant with "advice" in relation to his/her complaint. This is a new power, and it is not clear whether it would extend to providing a complainant with advice on the pursuit of civil remedies against a controller/processor.

New investigative powers/procedures - The DPC's new found power to impose substantial fines brings with it both additional investigative tools and balancing due process protections for those under investigation:

- Authorised officers will have enhanced powers to obtain and seek access to documents, including electronic records, and persons under investigation will be obliged to co-operate with the authorised officer.
- The authorised officer can oblige a person to answer questions under oath (Section 133(3)) and the authorised officer may decide to conduct a non-public oral hearing (Section 133(1)).
- After the investigation is completed, the authorised officer prepares a draft report, which is sent to the controller/processor for them to review/comment on within a 28 day period.
- The final report is then sent to the DPC, who may conduct further oral hearings/ investigations, before making a decision and/or exercising a corrective power.

One-stop-shop procedure – Section 108 of the Bill sets forth the Irish aspects of the procedure that will apply in circumstances where the DPC is the lead supervisory authority in a case that involves cross-border processing, commonly known as the "one-stop-shop" mechanism under the GDPR. A complicated procedure, involving an interaction between the lead supervisory authority, other concerned supervisory authorities and the European Data Protection Board (**the Board**), for such cases is described in Article 60 and Article 65 of the GDPR. The Bill addresses two important issues in relation to the operation of that procedure:

- Firstly, where the DPC is acting as the lead supervisory authority it shall conduct its investigation and exercise its powers in the same way as it does with standard investigations. The only difference is that it will reach a "draft decision" which it must then submit to other concerned supervisory authorities under the Article 60 co-operation procedure. The "draft decision" will address both the decision as to the complaint and, if applicable, "the envisaged action to be taken". Where a dispute arises under the co-operation procedure, the Board may make a binding decision (Article 65). At this stage the matter is remitted to the DPC, who makes a final decision on the question of infringement incorporating any revisions or guidance issued under the Article 60 and Article 65 processes.
- The second important issue addressed by the Bill is that it indicates that the Government has taken the view that the Board does not have authority to mandate the imposition of administrative fines or the exercise of other corrective powers by the DPC. The Bill as drafted splits one-stop-shop decision making into two stages. First a decision is made on the question of infringement by following the Article 60/65 procedure. The language of Section 108(2)(b) expressly recognises that this "infringement" decision may be revised by either the co-operation procedure (Article 60) or by a binding decision of the Board under Article 65.

  If, following this process, a decision is made to the effect that an infringement has occurred, a second decision is then required on whether to impose a sanction, and the extent of that sanction. Section 108(4) envisages the DPC making that "sanction" decision autonomously, without recourse to the Article 60 procedure for a second time. The only requirement is for the DPC to have "due regard" to revisions to envisaged corrective actions as may occur under the initial Article 60 procedure (Section 108(5)). The Bill appears to assume that the Board does

not have competency to make binding decisions in relation to the exercise of corrective powers under the Article 65 dispute procedure.

Representation of data subjects – The draft Scheme of the Bill published last year did not make provision for representative actions (sometimes called "class actions") to be taken, and there was considerable debate on this issue during the pre-legislative parliamentary scrutiny stage. The Bill has shifted significantly, but not completely, in favour of the representative action model. It permits a data subject to mandate a not-for-profit body to lodge complaints with the DPC. A mandated not-for profit body may also bring a civil claim on behalf of a data subject before the courts, however, it will not be able claim compensation on behalf of data subjects (Section 112(7)-(8)). In effect, therefore, the non-profit body will be able to seek injunctive relief, but not damages, on the data subject's behalf. The Bill does not address how the rules in relation to legal costs will apply to actions taken by non-profit bodies. In particular, guidance will be needed on whether a court can award costs against a data subject as well as the non-profit body in the event of an unsuccessful civil claim.

Appeal against an administrative fine or other corrective measure – The Bill provides that a decision of the DPC to exercise its corrective powers or to impose an administrative fine may be appealed to the Circuit Court (if the fine does not exceed €75,000) or to the High Court within 28 days of notice of the decision. On hearing the appeal, the Court may confirm the decision, replace it with another decision, or annul the decision (Sections 137 and 145).

Criminal Offences - The GDPR leaves it to national law to provide for any criminal offences in relation to infringements of the GDPR. The Bill provides for a number of offences, including: unauthorised disclosure by a processor; offences by directors etc. of corporate bodies; disclosure of personal data obtained without authority; enforced access requests; failure to cooperate with authorised officers during audit/inspections and investigations, and providing misleading information etc.

Publication of convictions, sanctions etc. – The Bill requires the DPC to publish particulars of convictions, and any exercise of its powers to impose fines or order the suspension of non-EEA transfers. It's a matter for the DPC to decide whether to publish particulars of the exercise of its other corrective powers (Section 144).

Privileged legal material – The Bill provides that where a controller or processor refuses to produce information to the DPC, or to grant access to it, on the grounds that the information contains privileged material, the DPC or an authorised officer may apply to the High Court for a determination as to whether the information is privileged material. The Court may then direct a person with suitable legal qualifications and expertise to examine the information and prepare a report to for the court to assist the court in determining whether the information is privileged legal material (Section 146).

KEY CONTACTS

John Whelan
Partner, Head of Commercial & Technology
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Mark Rasdale
Partner
+353 1 649 2300
mrasdale@algoodbody.com

Claire Morrissey
Partner
+353 1 649 2246
cmorrissey@algoodbody.com

Davinia Brennan
Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com