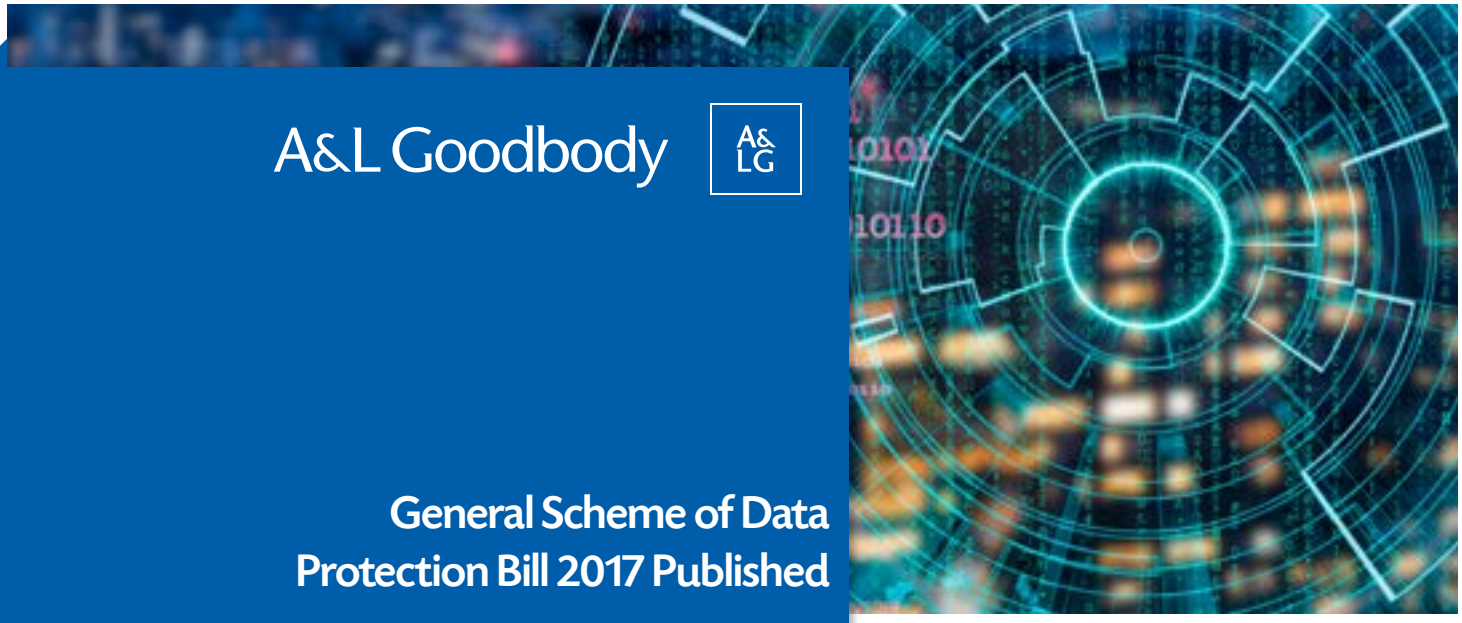
A&L Goodbody



General Scheme of Data Protection Bill 2017 Published

The Department of Justice and Equality have published the General Scheme of the Data Protection Bill 2017. This Bill is designed to give effect to, and provide for derogations from, the General Data Protection Regulation (**GDPR**). It also transposes the Law Enforcement Directive (2016/680) which concerns the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences, and the free flow of such data. The Bill is still at a preliminary stage and is likely to change considerably before it is enacted. In quite a few areas, the detail has been pushed into proposed secondary legislation. The most notable features of the Bill are the new powers and enforcement procedures (Part 5).

Important provisions of the Bill include:

Data Protection Commission: The Data Protection Authority is to become the *"Data Protection Commission"* (**DPC**), with the potential for up to three individual Commissioners to be appointed. This is to provide for additional capacity for dealing with the expected additional workload under the GDPR, and the *"one stop shop"* in particular. One Commissioner will be appointed as Chairperson.

Digital Age of Consent: The GDPR provides that where a child is below the age of 16 years, data processing shall only be lawful to the extent that consent is given or authorised by parents/guardians of the child. However, Member States have discretion to provide by law for a lower age, provided that such lower age is not below 13 years. The Government's consultation on this matter has closed, and the Bill contains an enabling provision for the age that is expected to be agreed shortly.

Freedom of Expression: The GDPR requires Member States to reconcile the right to protection of personal data with the right to freedom of expression. The Bill contains an exemption from many of the rights and obligations under the GDPR for processing that is done for journalistic purposes or the purposes of academic, artistic or literary expression, where compliance with the GDPR would be incompatible with the right to freedom of expression. It requires the right to freedom of expression to be *"interpreted in a broad manner"* and gives the DPC the power to refer any question of law to the High Court for determination. The explanatory note highlights that this broad exemption has been drafted with Article 11 of the Charter of Fundamental Rights in mind, which establishes a right to freedom of expression.

Derogations: The Bill grants broad ministerial powers, following consultation with the DPC, to restrict organisations' obligations and individuals' rights via regulations, in so far as necessary to *"safeguard important objectives of general public interest"*. The Bill contains a long non-exhaustive list of important public interest objectives, such as to safeguard national security, defence and international relations or to prevent threats to public security and safety. The Data Protection Acts 1988 and 2003 (**Acts**) contain broadly similar exemptions restricting individuals' rights for public interest reasons. However, as the obligations in the GDPR are set at a higher level, any restrictions imposed on the exercise of data subjects' rights will have to be justified at a corresponding higher level.

The Bill also restricts data subjects' rights (without the need for further regulations) in respect of processing:

- Data that is necessary for the establishment, exercise or defence of legal proceedings or other legal actions/claims, or the enforcement of civil law claims, including liability for damages or compensation;
- Opinions (concerning the data subject) given in confidence or on the understanding they would be treated as confidential; and
- Communications protected by legal advice or litigation privilege.

Organisations will welcome the legal privilege exemption as extending both to legal advice privilege (i.e. communications between a solicitor and client for the purposes of legal advice) and to litigation privilege communications (i.e. communications between a client and third party, or solicitor and third party, in anticipation of litigation).

Scientific, Historical Research or Statistics: The Bill also gives effect to Article 89 of the GDPR, which provides for derogations, subject to certain conditions, from specified data subject rights for processing for archiving purposes in the public interest, scientific, historical research or statistical purposes.

Criminal Convictions and Offences: The GDPR gives Member States discretion to legislate for the circumstances when criminal conviction data can be processed. The Bill identifies nine specific purposes on which the processing of data relating to criminal convictions and offences may be processed (without prejudice to the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 which allows certain minor offences to be disregarded after seven years). Helpfully, these purposes include, as separate grounds, where the processing is necessary for *"the assessment of risk or prevention of fraud"* and *"the establishment, defence or enforcement of civil law claims"*.

Special Categories of Data: The Bill provides for the making of ministerial regulations, following consultation with the DPC, permitting the processing of special categories of data (i.e. sensitive data) where *"necessary for reasons of substantial public interest"*. The Bill avails of the margin of flexibility afforded by the GDPR and specifies circumstances when processing of sensitive data is permitted under Irish law. It also expressly permits the processing of biometric data for identification and security purposes.

Designation of a Data Protection Officer: The GDPR requires the appointment of a DPO in certain circumstances, including: by public authorities and bodies; organisations whose core activities involve large scale processing of sensitive data or data relating to criminal convictions; and organisations whose core activities require regular and systematic monitoring of data subjects on a large scale. The GDPR provides a margin of flexibility for Member States by allowing them to enact national law that would require the appointment of a DPO in other cases, and the Bill creates a regulation-making power so that that flexibility can be availed of in the future.

Administrative Fines on Public Authorities and bodies: The Bill imposes fines on public authorities and bodies who are acting as *"undertakings"*. It appears, therefore, that fines will not be imposed on public bodies that do not have private sector competitors. An "undertaking" has the meaning given to it in section 3 of the Competition Act 2002. The explanatory note indicates that each activity of a public body will need to be evaluated separately when determining whether the public body is an *"undertaking"* and thus subject to administrative fines. A public body might be an *"undertaking"* for certain activities but not for others. For example, the HSE is an undertaking when it provides ambulance services to private patients, but not when providing the same service to public patients.

Investigative Powers: Greater investigative powers have been proposed for authorised officers of the DPC. In addition to the existing power of entry and power to take documents and records from data controllers/processors (subject to legal privilege), it is proposed that the DPC officers may call on individuals to provide *"reasonable assistance"* in relation to the operation of data equipment, including by providing passwords, and to attend before the DPC officers at a particular time and place, to provide relevant information &/or answer any questions. The DPC officers may also require a person to give their name and address for the purposes of the DPC applying for a search warrant. It will be an offence to obstruct or impede an officer, or to alter, destroy or refuse to provide any relevant information or give false or misleading information.

Search Warrants: There is a new general power proposed for a DPC officer, who has been prevented from entering premises, to apply for and execute a search warrant.

Privileged legal material: Where a controller/processor refuses to produce allegedly privileged material, the Bill provides that the DPC or an authorised officer can, within 28 days, apply to the High Court for a determination as to whether the information in question is privileged. The DPC or authorised officer must have reasonable grounds for believing the information does not contain privileged material, and reasonable grounds to suspect the information contains evidence relating to an infringement of the GDPR or this Act. The High Court may give directions regarding the appointment of a legally qualified person to examine and prepare a report for the court to assist it in determining whether the information is privileged.

Information or Enforcement Notices: As under the existing Acts, the Bill provides that it will be an offence to fail to comply with an information or enforcement notice, which will be punishable on summary conviction to a fine up to €5,000 or 12 months' imprisonment, or on conviction on indictment to a fine up to €50,000 or 5 years' imprisonment.

Right to an effective Judicial Remedy against DPC decisions/ notices: A statutory appeal may be brought within 28 days against an information or enforcement notice, or a legally binding decision of the DPC, or where the DPC has not dealt with a complaint, or does not inform the data subject within three months of the progress or outcome of the complaint.

Court Jurisdiction: It is proposed that the High Court will have concurrent jurisdiction with the Circuit Court to hear and determine appeals against information or enforcement notices and legal binding decisions of the DPC. At present, statutory appeals must be made to the Circuit Court.

DPC Urgent Court Application: It is proposed that the DPC will have the power to apply to the High Court to suspend or restrict the processing of personal data (including transfers to third countries) where there is an urgent need to protect the rights and freedoms of data subjects. This application can be made on an ex parte basis. In such cases, the DPC will be required to notify such measures, and the justification, to other concerned supervisory authorities, the European Commission and the European Data Protection Board (**EDPS**).

Power to Require Report: It is proposed that the DPC will have the power to require a controller or processer to prepare a report, in order to obtain relevant information for the purposes of an investigation or audit. It is envisaged that the *"report"* will be prepared be a *"reviewer"* nominated by the controller or processor and approved by the DPC or by a reviewer nominated by the DPC itself. It appears that the reviewer will have to act in an independent capacity. The explanatory note indicates that the Minister views this as an important new power and that it will be used in *"appropriate large-scale cases"*. It will be an offence to obstruct or impede a reviewer in preparation of a report; or to give false or misleading information to a reviewer; or for a reviewer to give false or misleading information to the DPC. The penalty will be a fine on summary conviction up to €5,000 &/or 12 months'

imprisonment, or on conviction on indictment to a fine up to €50,000 &/or 5 years' imprisonment.

Sanctions Procedure (Domestic Cases). It is proposed that the DPC will have the discretion to decide to conduct an oral hearing or alternatively to receive written submissions prior to imposing an administrative fine.

Sanctions Procedure (Cross-Border Cases): Where the DPC is acting as lead supervisory authority in a cross-border case, it is proposed that its draft decision will be submitted to other concerned supervisory authorities to allow for reasoned objections to be raised. Where there is a dispute between the DPC and the other supervisory authority(s), the matter is referred to the EDPB for resolution. It appears that the discretionary written submissions/oral hearing procedure will take place before the draft decision is sent to the other supervisory authorities.

Administrative Fine Appeals: A controller or processor has up to 30 days, from the date on which the notice of the decision was served, to appeal a decision of the DPC to the High Court or to the Circuit Court if the fine amounts to less than €75,000. The courts have jurisdiction to hear any evidence, even if not already made to an authorised officer or the DPC.

Confirmation of Administrative Fines. The DPC is required to apply to the Circuit Court to confirm any administrative fine decision, after the expiration of 30 days, even when there is no appeal. The court will confirm the decision unless it sees good reason not to do so. This is a normal feature of Irish administrative fine legislation, as it is a recognised constitutional requirement, to ensure the decision is taken in line with procedural rules and constitutional justice.

Unauthorised disclosure by a processor – The Bill contains a similar provision to the existing Acts, specifically prohibiting disclosure of personal data by a processor, employee or agent, without the prior authority of the data controller and makes such disclosure an offence. On summary conviction a person may be subject to a fine up to €5,000 &/or 12 months' imprisonment, or on conviction on indictment to a fine up to €50,000 &/or imprisonment for a term not exceeding 5 years.

Director liability. As under the current Acts, the Bill imposes personal liability on a director, manager, secretary or other officer, as well as the body corporate, where an offence is committed by the body corporate and is proved to have been committed with the *"consent or connivance of, or to be attributable to any neglect"* of such persons.

Prosecution of summary offences by the DPC: The DPC has 3 years from the date an offence is alleged to have been committed to prosecute a person. If the person is outside Ireland during that 3 years, then the DPC has a further 6 months from his/her return to Ireland to prosecute. However, no person may be prosecuted after 5 years from the date of the offence.

Publication of convictions, sanctions etc. The DPC must publish details of convictions, administrative fines and any suspensions of data transfers. The DPC may also publish particulars of any report by the DPC of investigations or audits it has carried out.

Judicial Remedy for data subjects: It is proposed that data subjects will have direct access to the courts to obtain both monetary awards and injunctive relief. A judicial remedy may be sought whether or not the data subject has lodged a complaint with the DPC.

Immunity of DPC from suit: The Bill provides that there is no right to bring civil or criminal proceedings against the DPC or its staff in respect of anything said or done in good faith in the course of their functions. There is no equivalent provision in the existing Acts.

Limitation on international transfers outside the EEA: The Bill enables the Minister for Justice, in the absence of an adequacy decision, and following consultation with any relevant Minister and the DPC, to make regulations restricting the transfer of *"specific categories"* of personal data to a third country or international organisation *"for important reasons of public interest"*.

CJEU Reference Procedure: A procedure for seeking references to the CJEU in line with the requirements of the Schrems case is proposed. The Bill enables the DPC to apply to the High Court, where it considers a third country or international organisation to which personal data are transferred does not provide an adequate level of protection, for a determination as to whether the level of protection is adequate, or for an order referring the matter to the CJEU. The DPC may also apply to the High Court for a determination or CJEU referral where it is of the opinion that the standard contractual clauses do not ensure an adequate level of protection. Only the CJEU can annul an adequacy decision.

KEY CONTACTS

For further information please contact one of our IP & Technology Partners below:

John Whelan
Partner
T: +353 1 649 2234
E: jwhelan@algoodbody.com

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

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

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