A&L Goodbody

# Ireland passes Data Protection Act 2018

The Irish Data Protection Act 2018 was signed into law on 24 May 2018, to coincide with the coming into effect of the GDPR. The Act implements derogations permitted under the GDPR and represents a major overhaul of the regulatory and enforcement framework. At the final parliamentary stages, some unexpected changes were made to the Act. This briefing note analyses the key provisions under the Act and its likely impact on businesses operating from Ireland.

## Key provisions and amendments


- Setting the digital age of consent at 16 years
- Enabling a not-for-profit body (mandated by a data subject) to bring a civil action seeking compensation and injunctive relief on behalf of the data subject for a breach of data protection law
- Providing that any reference to "child" in the GDPR shall be taken to be a person under 18 years (other than in regard to Article 8 of the GDPR)
- Making it an offence, punishable by an administrative fine, to process the personal data of a child under 18 years of age for the purposes of direct marketing, profiling or micro-targeting
- Providing a specific right to be forgotten for children requiring a controller, on request, to erase personal data collected in relation to the offer of information society services to a child
- Requiring the Irish Data Protection Commission (DPC) to encourage the drawing up of codes of conduct to ensure the proper application of the GDPR with regard to children
- Enabling administrative fines of up to €1 million to be imposed on public bodies or public authorities that do not act as undertakings (i.e. that are not in competition with private sector bodies)
- Providing restrictions on individuals' rights on the grounds of legal privilege, for archiving, scientific or historical research purposes or statistical purposes, and in other specified circumstances for important objectives of general public interest
- Providing new investigative and enforcement powers for the DPC, including enhanced search and seizure powers, the appoint of expert reviewers, the drawing up of investigation reports, examining witnesses under oath and conducting oral hearings
- Permitting the processing of personal data and special categories data for a purpose other than that for which it was collected where necessary and proportionate: to prevent threats to national security; investigate or prosecute criminal offences, or for legal advice or legal proceedings
- Providing a derogation for the right to freedom of expression and information which must be interpreted in a broad manner
- Permitting the processing of health data for insurance and pension purposes
- Permitting the processing of personal data relating to criminal convictions and offences in specified circumstances
- Establishing a number of criminal offences punishable by a fine of up to €5,000 and/or 12 months imprisonment on summary conviction, or up to €250,000 and/or 5 years' imprisonment on conviction on indictment

## Overview of the Act

The Data Protection Act 2018 was signed into law on 24 May 2018, and some of the provisions will take effect on 25 May 2018, so as to coincide with the coming into force of the GDPR. The late publication of this lengthy and complex Act, which runs to 232 sections and 174 pages, means businesses now have little time to digest their new obligations. The Data Protection Act, 1988, as amended, shall continue to apply to a complaint by an individual under section 10 of that Act, and to any contravention of that Act, that occurred before 25 May 2018. In addition, an investigation under section 10 that has begun but not completed prior to 25 May 2018 shall be completed in accordance with that Act.

The Act has five key elements:

1. It repeals the Data Protection Act 1988, as amended, except those provisions relating to the processing of personal data for the purposes of national security, defence, and international relations of the State.
2. It transposes the Law Enforcement Directive which regulates the processing of personal data by law enforcement authorities.
3. It provides, in the limited areas permitted, for national derogations from the obligations set out in the GDPR.
4. It contains new enforcement powers and mechanisms for the DPC.
5. Due to the entry into force of the GDPR and this Act, it provides for a number of amendments to sixty-five other Acts of the Oireachtas, as well as revoking a number of statutory instruments.

This briefing focuses on the key derogations in the Act and the new regulatory framework.

## National Derogations

**Child for the purposes of the GDPR -** The Act provides that references to "child" in the GDPR shall be taken to refer to a person under 18 years of age. This is in line with the definition in Article 1 of the UN Convention on the Rights of the Child (section 29).

**Digital age of consent –** The Act provides that 16 years is the minimum age at which a child may consent to the processing of their personal data by information society service providers. The consent of the child's parent of guardian will be required by information society service providers in regard to children under that age. The European Court of Justice recognises "information society services" as covering contracts and other services that are concluded or transmitted on-line. Throughout the legislative process the Government had advocated 13 years of age as the "digital age of consent" but, in the end, the opposition parties defeated the Government on this issue (section 31). The Act provides for a review of the operation of this provision not later than 3 years after its commencement.

**Micro-targeting and profiling of children –** The Act provides that it will be an offence, punishable by an administrative fine, for a company to process the personal data of a child under 18 years of age for the purposes of direct marketing, profiling or micro-targeting. Once again the opposition parties defeated the Government, by requiring the introduction of this provision. This provision is aimed at prohibiting companies from harvesting children's data and profiling children for direct marketing and commercial purposes. However, there are concerns that Ireland may be in breach of EU law by enacting this provision, insofar as it imposes limitations in national law on the processing of personal data that is lawful under the GDPR. Minister Flanagan highlighted that the processing of personal data for marketing and profiling purposes may take place on the "legitimate interests" ground in Article 6(1)(f) of the GDPR, and recital 47 states this particularly. Minister Flanagan has indicated that he has formally requested legal advice from the Office of the Attorney General on the legality of including this provision, and that in the meantime, it may be necessary to delay or defer commencement of this provision (section 30).

**Codes of Conduct: Children –** The Act requires the DPC to encourage associations and other bodies representing categories of controllers or processors to draw up of codes of practice to contribute to the proper application of the GDPR with regard to the protection of children, the manner in which the consent of holders of parental responsibility over a child is to be obtained by information society services providers, and with regard to the processing of children's data for direct marketing and profiling purposes. This provision is permitted by Article 40 of the GDPR (section 32).

**Right to be forgotten: Children –** The Act provides a specific right to erasure for children in regard to personal data collected in relation to the offer of information society services. This provision seems unnecessary insofar as Article 17(1)(f) of the GDPR already provides for a right of erasure in these circumstances. Repeating the text of the GDPR in national law is prohibited, unless such repetitions are strictly necessary for the sake of coherence (Recital 8 GDPR). The Act further provides that the right to erasure will not apply to the extent that the processing is necessary for the purposes set out in

Article 17(3) of the GDPR, such as where processing is necessary for compliance with a legal obligation or the defence of legal claims (section 33).

**Data Protection Officers –** The Act allows the Minister, in consultation with the DPC, to extend the categories of controllers and processors that are required to designate a data protection officer, as permitted by Article 34(7) of the GDPR (section 34).

**Brexit Derogation –** The Act permits the processing and disclosure of personal data where the controller is an airline or ship for the purposes of preserving the Common Travel Area. The Act gives the Minister power to make regulations for the purposes of specifying the part of the Common travel Area to which the regulations apply, and the personal data than may be processed. The provision appears to be addressing the risk of potential interruptions to air and sea travel post-Brexit (section 38).

**Further Processing –** The Act permits the processing of personal data and special categories of personal data (i.e. data relating to health, race or ethnic origin, trade union membership, political, religious or philosophical beliefs) other than for the purpose for which it was collected, where such processing is necessary and proportionate for the purpose of: (i) preventing a threat to national security; (ii) preventing, detecting, investigating or prosecuting criminal offences; or (iii) providing legal advice or legal proceedings (section 41). Certain statutory provisions permit or require further notification or disclosure of personal data, such as anti-money laundering legislation which requires designated persons to report any knowledge or suspicion of money laundering to the Gardaí and the Revenue Commissioners.

**Processing for archiving in the public interest, scientific or historical research purposes or statistical purposes –** The Act confirms that personal data and special categories of 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 42 & 54).

**Data processing and freedom of expression –** The GDPR requires Member States 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 Act 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 Act provides that the right to freedom of expression shall be interpreted in a broad manner (section 43).

**Communicating with and representing the electorate –** The Act contains enables political parties, candidates and holders of political offices to communicate in writing (including by way of newsletter or circular) with data subjects during the course of electoral activities in the State. It also provides that elected representatives may lawfully process personal and special categories of data of data subjects, to enable them to act on behalf of a data subject when they receive a request to do so. It shall also be lawful for a third party to disclose to a representative personal and special categories of data relating to a data subject on whose behalf the request is made (sections 39-40). In addition, the Act permits the processing of personal data revealing political opinions in the course of electoral activities in the State for the purpose of compiling data on people political opinions by a political party, candidates for electoral office, or by the Referendum Commission (section 48).

**Restriction of right to object to processing for electoral activities -** The Act restricts the rights of data subjects to object to direct marketing by post where it is carried out in the course of electoral activities in the State. It also restricts the right to object to processing of personal data when such processing is carried out in the course of electoral activities in the State, by political parties or candidates for electoral office, or by the Referendum Commission. These restrictions are carried over from the Data Protection Act 1988, as amended. Existing restrictions on electoral activities carried out by electronic means without the consent of individuals under the e-Privacy Regulations 2011 are not affected (sections 58-59).

**Processing of special categories of personal data –** Article 9 of the GDPR gives Member States some discretion in regard to the lawful bases to legitimise the processing of special categories of data. The Act permits special categories of data to be processed for a limited number of purposes, including: for employment purposes (section 46); health-related purposes (sections 52-53); providing legal advice and legal proceedings (section 47); and the administration of justice and performance of a function conferred by an enactment or by the Constitution (section 49). The Act also creates a regulation-making power whereby regulations may be made in the future permitting the processing of special categories of personal data for reasons of substantial public interest (section 51).

**Processing of health data for insurance and pension purposes –** The Act permits the processing of health data where it is necessary and proportionate for the purpose of policies of insurance or life assurance, health insurance or health-related insurance, pensions or the mortgaging of property. The motivation behind this provision is to address difficulties arising from the strict definition of "consent" in the GDPR. The government, like other Member States, recognised that difficulties arose with insurance companies and financial institutions seeking to rely on the explicit consent of a data subject under Article 9(2)(a) to legitimise their processing of health data, as the definition of "consent" in the GDPR requires that for the consent to be valid, it must be "freely given" (section 50).

**Suitable and specific measures for processing –** The Act requires certain processing activities to be subject to the implementation of "suitable and specific measures" to safeguard the fundamental rights and freedoms of data subjects. Section 36 of the Act contains a "toolbox" of measures for application in such cases (e.g. strict time limits for erasure of personal data or specific targeting training for those involved in processing operations). The Act also provides the Minister with power to make future regulations identifying additional "suitable and specific measures", or to specify that a particular measure is mandatory in respect of certain processing.

**Processing of personal data relating to criminal convictions and offences –** The Act gives effect to Article 10 of the GDPR, which permits personal data relating to criminal convictions and offences to be processed under the control of official authority or for specified purposes under national law. The Act provides examples of processing under official authority (e.g. for the administration of justice) and specifies five purposes where processing is permitted under the Act, including: (i) where the data subject has given explicit consent; (ii) where the processing is necessary for the performance of a contract to which the data subject is a party; (iii) for the purpose of legal advice, legal proceedings or defending legal claims; (iv) to prevent injury or other damage to the data subject or another person or loss or damage to property, or (v) further to Ministerial regulations or other statute. This provision is without prejudice to the provisions of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016 (section 55).

**Restrictions on individuals' rights –** Article 23 of the GDPR permits Member States to restrict the exercise of individuals' rights and controllers' obligations in certain circumstances, for the purpose of safeguarding important objectives of general public interest. Section 60 of the Act is an important provision, which sets out a number of restrictions. Individuals' rights and controllers' obligations are restricted to the extent necessary and proportionate:

- to safeguard cabinet confidentiality, parliamentary privilege, national security, defence and the international relations of the State
- for the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties
- for the administration of any tax, duty or other money due or owing to the State or a local authority in any case in which the non-application of the restrictions concerned would be likely to prejudice the aforementioned administration
- in contemplation of or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure
- for the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim
- for the purposes of estimating the amount of the liability of a controller on foot of a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of those rights or obligations would be likely to prejudice the commercial interests of the controller in relation to the claim, or
- to protect personal data relating to a data subject which consist of an expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential.

The Act gives the Minister power to make future regulations further restricting individuals' rights and controllers' obligations where necessary for important objectives of general public interest.

**Legal Privilege -** The Act also restricts the rights of individuals and obligations of controllers in regard to documents which are protected by legal privilege. The Act provides a broad exemption for privileged documents, similar to that available at

common law. It protects from disclosure all "(i) personal data processed for the purpose of seeking, receiving or giving legal advice or (ii) personal data in respect of which a claim of privilege could be made for the purpose of, or in the course of legal proceedings, including personal data consisting of communications between a client and his or her legal advisers or between those advisers, or (iii) where the exercise of such rights or performance of such obligations would constitute a contempt of court" (section 162).

**Restrictions on individuals rights for archiving, scientific or historical research purposes or statistical purposes –** The Act provides that certain rights of individuals (including the right of access, rectification, restriction of processing and right to object) may be restricted to the extent that the exercise of those rights would be likely to render impossible, or seriously impair the achievement of those purposes, and the restriction is necessary for the fulfilment of those purposes (section 61).

## New Regulatory Framework

The Act represents a radical overhaul in regard to the way in which complaints, investigations and enforcement actions will be handled by the DPC. The Act contains twenty-five sections dealing with the DPC's enforcement and investigation powers (Part 6, Chapters 2, 4 & 5), along with additional provisions dealing with administrative fines and criminal offences (Part 6, Chapters 6 & 7). These lengthy provisions reflect the fact that the DPC now wields a powerful array of corrective powers.

### Handling Complaints

The Act grants the DPC more discretion in regard to handling complaints from data subjects, or not-for-profit bodies acting on their behalf (Chapter 2). Under the Data Protection Act 1988, as amended, the DPC is required to investigate all complaints and seek an amicable resolution. A complaint can only be rejected on the grounds that it is frivolous or vexatious, which is only available in the most narrow circumstances. In contrast, the Act requires the DPC to examine all complaints and to take such action as it considers appropriate, having regard to the nature and circumstances of the complaint. The DPC can only refuse to act on a complaint when it is manifestly unfounded or excessive, in particular because of its repetitive character which shall apply only in the narrowest of circumstances (Article 57(4) GDPR).

### Amicable Resolution

If the DPC considers there is a "reasonable likelihood" of the parties reaching an amicable resolution of the complaint, the DPC may arrange or facilitate such a resolution. Once a resolution has been reached, the complaint will be deemed to have been withdrawn by the complainant, and no formal statutory decision will be required.

### Other Actions

Where the DPC considers than an amicable resolution cannot be reached in the case of a domestic complaint, it must take one or more of the actions (section 109):

(i) Reject the complaint

(ii) Dismiss the complaint

(iii) Provide advice to the data subject in relation to the complaint

(iv) Serve an enforcement notice requiring the controller or processor to take certain actions to comply with data protection law

(v) Conduct an inquiry into the complaint (i.e. investigate the complaint), or

(vi) Take such other action as it considers appropriate.

Where the DPC considers that an amicable resolution cannot be reached in relation to a complaint concerning cross-border processing, in respect of which the DPC is the lead authority, it must follow the "one-stop-shop procedure" set out in section 113 of the Act (see "One-Stop-Shop Procedure" below).

The DPC must notify the complainant in writing of the action it is taking as soon as practicable, and at the latest within 3 months of receipt of the complaint (section 108).

### Conducting an Inquiry

The DPC may conduct an inquiry into a suspected infringement arising out of a complaint, or an inquiry of the DPC's own volition (there is no requirement to establish a probable cause). In conducting its inquiry, the DPC may exercise any of its powers under Part 6, Chapter 4 (other than the power to require an expert report pursuant to section 135) and/or carry out an investigation under Chapter 5 (section 110).

The Chapter 4 investigation pathway is for where the DPC decides that an authorised officer needs to be appointed to conduct an investigation using its search and seizure, audit or enforcement powers (e.g. serving an information or enforcement notice), but where the DPC does not (initially at least) intend to impose an administrative fine sanction.

The Chapter 5 investigation pathway is for where the DPC considers that an in-depth investigation is required, with the option of imposing an administrative fine. It involves a quasi-judicial inquiry, with due process protections added. The DPC may appoint an authorised officer who can examine witnesses under oath, order the production of documents and, where necessary, conduct oral hearings in private.

**Chapter 4 Investigation Powers**

Chapter 4 of the Act provides authorised officers with broad powers to enter business premises unannounced and without a court ordered search warrant. Court ordered search warrants are only required in regard to private dwellings or where an authorised officer is prevented access to business premises. It is an offence to obstruct or impede an officer or to refuse to comply with a request by the officer, or to alter, suppress or destroy any information which the officer may reasonably require.

Authorised officers may search and inspect the premises and any information found there, and secure for later inspection any information or equipment. They may remove and retain documents for such period as the authorised officer reasonably considers necessary for the purposes of the performance of his or her functions. Employees may be required to produce any documents relating to the processing of personal data that are within that person's power or control, and provide authorised officers with any passwords necessary to enable them to access and examine documents (sections 130 & 131).

The controller or processor can refuse to produce legally privileged documents, but must preserve the information pending an application by an authorised officer or DPC to the High Court for a determination as to whether the information is privileged. The court may direct a person with suitable legal qualifications and expertise to examine information and prepare a report to assist the court in making its determination (section 151).

Information and enforcement notices may be issued by an authorised officer or the DPC, requiring a controller or processor, to provide certain information or take specified steps. As under the Data Protection Act 1988, as amended, it is an offence to fail to comply with these notices. A controller or processor has the right to appeal any notice to the High Court within 28 days of receipt of the notice (sections 132 & 133).

Where there is a need to act urgently in order to protect data subjects, the DPC may apply to the High Court for an order suspending, restricting or prohibiting data processing operations, or the transfer of data to a third country (section 134).

The DPC has further powers that may be exercised outside of a formal investigation, for the purpose of monitoring compliance with the GDPR, including requiring a controller or processor to provide a report on a matter specified by the DPC. The report would be prepared by an expert nominated by the controller or processor concerned, and approved by the DPC. Before requiring such a report, the DPC will be required to consider whether any other powers may be exercised which may be more appropriate in the circumstances, the level of resources available to the controller or processor, and the likely benefit to the controller or processor of providing the report (section 135). The explanatory memorandum notes that the DPC's power of require a report is broadly based on powers already available to the Central Bank of Ireland under Part 2 of the Central Bank (Supervision and Enforcement) Act 2013.

In addition, the DPC may carry out an investigation in the form of a data protection audit in order to ascertain whether the practices and processes of a controller or processor are in compliance with the GDPR. The Act requires the DPC to give the controller or processor concerned at least 7 days' notice of its intention to commence an audit (section 136).

**Chapter 5 Investigation Powers**

Chapter 5 of the Act sets out a quasi-judicial procedure for conducting in-depth investigations into possible infringements of the GDPR. It provides for separate investigative and adjudicative stages in an investigation. The DPC may appoint one or more authorised officers to undertake the investigation and to submit to the DPC an investigation report following completion of the investigation (section 137).

For the purposes of an investigation, an authorised officer may order the production of documents, require a person to attend before the officer to answer any questions under oath, and may decide to conduct a private oral hearing. It will be an offence to withhold, destroy or refuse to provide any information for the purposes of an investigation or to obstruct an authorised officer (section 138).

Having completed an investigation, an authorised officer will be required to prepare, in writing, a draft investigation report setting out his or her findings, which will be sent to the controller or processor for them to make written submissions on within a 28 day period. On the expiration of that period, an authorised officer, having regard to any submissions made by the controller or processor, will prepare a final report for submission to the DPC. The investigation report shall state whether the authorised officer is satisfied or not that an infringement has occurred and why. However, the authorised officer is not empowered to make any recommendation in regard to any sanction that ought to be imposed by the DPC. That is a matter entirely reserved for the DPC (section 139).

On receipt of the report, the DPC will consider its contents, including any submissions attached to it. If further information is required, the DPC may conduct an oral hearing, seek further submissions from the controller or processor, or require the authorised officer to carry out further investigations (section 140).

The DPC must then reach a formal decision as to whether it is satisfied that an infringement has occurred, and if so whether to exercise a corrective power. The DPC is required to give the controller or processor a notice in writing setting out the decision and the reasons for it, and the corrective power it has decided to exercise, which may result in an administrative fine being imposed (section 116).

**Imposition of fines on public bodies and authorities**

The Act permits the DPC to impose administrative fines of up to €1 million on public bodies or public authorities that do not act as undertakings within the meaning of the Competition Act 2002 (i.e. that are not in competition with private sector bodies) (section 141).

**Appeal against an administrative fine or other corrective measure**

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 the High Court. On hearing the appeal, the Court may confirm, replace or annul the decision (section 142 & 150).

If the appeal is not lodged within 28 days, the controller or processor will have lost its right of appeal and the DPC can then apply to the Circuit Court (irrespective of the amount of the fine) to have the administrative fine confirmed. The purpose of this confirmation mechanism, is to ensure than any decision to impose an administrative fine has due regard to fair procedures and constitutional justice (section 143).

**One-Stop-Shop Procedure**

Section 113 of the Act 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 Act 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 Act 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 Act splits the 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 113(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 113(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 113(5)). The Act 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 Bill, as initiated, provided that a data subject could mandate a not-for-profit body to lodge complaints with the DPC on its behalf. That body could also take a representative action before the courts seeking injunctive relief, but could not seek compensation on behalf of the data subject. The issue of representative actions was the subject of much controversy throughout the legislative process, and the Act now permits a mandated not-for-profit body to bring a representative action on behalf of a data subject seeking injunctive relief or compensation for material or non-material damage suffered as a result of an infringement of data protection law (section 117). It remains to be seen whether this means not-for-profit bodies will be able to take class actions on behalf of multiple data subjects for breaches of the GDPR, as such actions are not currently permitted under Irish law.

The Act does not address how the rules in relation to legal costs will apply to actions taken by not-for-profit bodies. In particular, guidance will be needed on whether a court can award costs against a data subject as well as the not-for-profit body in the event of an unsuccessful civil claim.

**Criminal Offences**

The GDPR leaves it to Member States to provide for any criminal offences in relation to any infringements of the GDPR. Under the Act, the DPC will continue to have the power to prosecute controllers and processors for summary offences in the District Court (Section 147). The maximum penalty for summary offences under the Act is a Class A fine (i.e. €5,000) and/or 12 months' imprisonment. Indictable offences will be prosecuted by the DPP in the Circuit Court or Central Criminal Court. The maximum penalty for an indictable offence under the Act is €250,000 and/or 5 years' imprisonment, depending on the nature of the offence.

The Bill, as initiated, provided that the DPC cannot impose an administrative fine on a controller or processor where it has been subject to criminal penalty in respect of the same act or omission (the *"ne bis in idem"* rule). Although this provision was deleted at Committee Stage of Dáil Éireann, it should not be possible for a controller or processor to be sanctioned by both a criminal penalty and an administrative fine for the same infringement, as pursuant to Article 84 of the GDPR, national law may only provide for penalties applicable to infringements of the GDPR which are not already subject to administrative fines.

The Act sets out a number of criminal offences including:

- **Enforced Access Requests –** It is an offence for a potential or current employer to require a data subject to make a data access request to a specified person or to require a data subject to supply any information obtained as a result of such a request (section 4).
- **Unauthorised disclosure by processor –** It is an offence for a processor, or an employee or agent of the processor, to knowingly or recklessly disclose personal data being processed on behalf of a controller without the prior authority of the controller, unless the disclosure is required or authorised by any enactment, rule of law or court order (section 144).
- **Disclosure of personal data obtained without authority –** It is an offence for a person to obtain and disclose personal data to a third party without the prior authority of the controller or processor, unless the disclosure is required or authorised by any enactment, rule of law or court order. It is also an offence for a person to sell or offer to sell personal data that were unlawfully disclosed to or obtained by him/her (section 145).
- **Offences by directors etc. of bodies corporate –** Where an offence under the Act is committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of a person being a director, manager, secretary, or other officer of that body, or a person purporting to act in such capacity, that person, as well as the body corporate shall be guilty of the offence and liable to be punished as if he/she were guilty of the first-mentioned offence (section 46).
- **Knowingly or recklessly processing data relating to criminal convictions or offences –** It is an offence to knowingly or recklessly process personal data relating to criminal convictions or offences in contravention of the processing conditions set down in the Act (section 55(8)).

- **Failure to co-operate with authorised officers during inspections, audits, and investigations** – The Act provides for a number of offences in relation to obstructing an authorised officer in the performance of his or her functions (sections 130(7) & 138(12)).
- **Failing to comply with an information or enforcement notice –** It is an offence to fail to comply with a statutory information or enforcement notice served by the DPC (sections 132(6) & 133(10)).
- **Obstructing a reviewer in the preparation of a report –** It is an offence to obstruct an expert in the preparation of his/her report or to give him/her false or misleading information (section 135(15)).

**Publication of convictions, sanctions etc.**

The Act 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, or court orders suspending, restricting or prohibiting data processing operations. It's a matter for the DPC to decide whether to publish particulars of the exercise of its other corrective powers. The DPC may also publish, if it considers it in the public interest to do so, any expert report under section 135, or any investigation or audit report (Section 149).

## 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**
*Associate & Knowledge Lawyer*
+353 1 649 2114
dbrennan@algoodbody.com