COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Ireland

DATA PROTECTION & CYBER SECURITY LAW

Contributing firm

ByrneWallace LLP

Jon Legorburu

Partner and Head of Litigation and Dispute Resolution | jlegorburu@byrnewallace.com

Seán O'Donnell

Partner, Litigation and Dispute Resolution/Privacy & Data Protection | sodonnell@byrnewallace.com

Zelda Deasy

Partner, Corporate/Privacy & Data Protection | zdeasy@byrnewallace.com

This country-specific Q&A provides an overview of data protection & cyber security law laws and regulations applicable in Ireland.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

IRELAND
DATA PROTECTION & CYBER SECURITY LAW

1. Please provide an overview of the legal and regulatory framework governing data protection and privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the relevant laws). Are there any expected changes in the data protection and privacy law landscape in 2022-2023 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

The primary legislation governing data protection and privacy in Ireland is the Data Protection Act 2018, as amended, (the "**Act**"), which gives further effect to the General Data Protection Regulation ("**GDPR**") and transposes Directive (EU) 2016/680 (the "**Law Enforcement Directive**") which applies to the processing of personal data for law enforcement purposes. The Data Protection Acts 1988 and 2003 still apply in certain circumstances, such as to the processing of personal data for the purposes of safeguarding the security of the State.

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the "**e-Privacy Regulations**") transpose Directive 2002/58/EC (the "**e-Privacy Directive**") into Irish law. The e-Privacy Regulations outline specific rules with regard to the use of cookies, marketing communications and security of electronic communications networks and services.

The Data Sharing and Governance Act 2019 (the "**2019 Act**") introduced requirements for the sharing of information, including personal data, between public bodies, provided for the establishment of base registries and the Personal Data Access Portal, and established the Data Governance Board (the "**Board**"). The 2019 Act has been introduced in successive phases, the final of which comes into effect on 16 December 2022.

The Data Protection Commission (the "**DPC**") is the national competent authority for the regulation and enforcement of data protection and privacy law in Ireland.

2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?

There are no registration or licensing requirements for controllers or processors in Ireland. All organisations that have appointed a Data Protection Officer ("**DPO**") pursuant to the GDPR are required to notify the contact details to the DPC, which holds a register of DPOs.

3. How do these laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?

Personal data is defined in the GDPR as any information relating to an identified or identifiable natural person ('data subject'); an identifiable person being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special category data means genetic data, biometric data for the purposes of uniquely identifying an individual, data concerning health; an individual's sex life or sexual orientation, or personal data revealing the racial or ethnic origin of the data subject; the political opinions or the religious or philosophical beliefs of the

data subject; or whether the data subject is a member of a trade union.

The Act also adopts the GDPR definitions of biometric data, genetic data and data concerning health, as well as the key definitions set out in Article 4 of the GDPR e.g. processor, controller and processing.

The definition of personal data in the 2019 Act extends to cover deceased individuals.

4. What are the principles related to, the general processing of personal data or PII – for example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction or must personal data or PII only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

In Ireland, those who process personal data have to demonstrate compliance with the principles of GDPR as follows:

a. Lawfulness, fairness and transparency: processing must have a legal basis and not be unlawful, must not be misleading, unexpected or deceptive and done in a transparent manner in relation to the data subject.
b. Purpose limitation: personal data must be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes.
c. Data minimisation: processing of personal data must be strictly limited to what is necessary and relevant to accomplish a specified purpose. Data should be retained only for as long as is necessary to fulfil that purpose.
d. Accuracy: controllers must ensure that personal data are accurate and, where necessary, kept up to date; controllers must consider that inaccurate data must be deleted.
e. Storage limitation: personal data must not be retained for longer than is necessary for the purposes for which the personal data are processed.
f. Integrity and confidentiality: personal data should be processed in a manner that ensures appropriate security and confidentiality.
g. Accountability: the controller is responsible for, and must be able to demonstrate to the DPC, their compliance with all principles of data protection described above.

Irish law also requires that processing must be established on one of the six legal bases for processing provided by Article 6 of the GDPR, i.e. consent, performance of a contract, a legitimate interest, a vital interest, a legal obligation or a public task.

5. Are there any circumstances where consent is required or typically used in connection with the general processing of personal data or PII?

Under Irish law, explicit consent is required for the use of data for health research purposes pursuant to the Data Protection Act 2018 (Section 36(2)) (Health Research) (Amendment) Regulations 2018, 2019 and 2021.

Pursuant to the e-Privacy Regulations, consent is required in respect of electronic direct marketing for new customers. Consent is not required in respect of electronic direct marketing for existing customers, where certain conditions are satisfied.

Consent is necessary for the use of non-necessary cookies (see question 20 below).

Consent is often the most appropriate basis for the use of biometric data.

6. What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

In order for consent to be valid under the GDPR it must be freely given, unambiguous and fully informed. It must be specific to the data processing in question and distinguished from other matters when requested. Data subjects must give an unambiguous indication of their agreement to the data processing operations, by a clear affirmative act. Silence, pre-ticked boxes or inactivity will not suffice.

In order to ensure that consent is freely given, controllers should avoid using consent as the legal basis for processing where there is a clear imbalance of power between the data subject and the controller.

The GDPR expressly provides for the right of a data subject to withdraw his/her consent at any time and requires consent to be as easy to withdraw as to give in the first place.

7. What special requirements, if any, are required for processing sensitive PII? Are there any categories of personal data or PII that are prohibited from collection?

Processing special category personal data is prohibited, except in limited circumstances as prescribed by Article 9 of the GDPR and the Act, for example where there is explicit consent, or where it is necessary for the purposes of public interest in the area of public health.

Additional restrictions apply where the data is processed for law enforcement purposes.

8. How do the laws in your jurisdiction address children's personal data or PII?

Data protection legislation in Ireland applies to all living individuals, regardless of their age. In December 2021, the DPC published "Fundamentals" on the processing of children's personal data, which introduce child-specific data protection interpretative principles and recommended measures to enhance the level of protection afforded to children against the data processing risks posed to them by their use of/access to services both online and offline.

The digital age of consent in Ireland is 16, meaning that a child aged 16 or over can provide their consent in relation to the offer of information society (or distance) services. If the child is younger than 16, the holder of parental responsibility must have given or authorised the consent.

The Act creates an offence for a company or corporate body to process the personal data of a child for the purposes of direct marketing, profiling, or micro-targeting. At the time of writing, this section has not been commenced.

9. Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.

The GDPR and the Act set out various derogations, exclusions and limitations, for example in relation to data subject rights. The Act permits controllers to restrict data subject rights where it is necessary and proportionate to safeguard certain objectives, as outlined under section 60 of the Act. These objectives include, inter alia, to safeguard national security, for the purposes of criminal prosecutions, to enforce civil claims and to protect legally privileged information.

The Data Protection Act 2018 (Access Modification) (Health) Regulations 2022 restrict data subject access to health data, where the application of that right would be likely to cause serious harm to the physical or mental health of the data subject.

Derogations also exist in relation to the transfer of data outside the EEA.

10. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

Both "Data Protection by Design" and" Data Protection by Default" are part of the Irish legal system under Article 25 of the GDPR. The Irish regime does not impose specific domestic requirements in this regard. Organisations are responsible for deciding on the measures appropriate to comply with these requirements, in light of the type of processing activities which they carry out.

11. Are owners or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.

Article 30 of the GDPR imposes a duty on controllers, processors and their representatives to record data processing activities. The records of processing activities must be submitted to the DPC upon request. These records must be in writing, including electronic form, and must be regularly updated. Companies or institutions with fewer than 250 employees are exempt from keeping a record in certain circumstances.

12. Do the laws in your jurisdiction require or recommend having defined data

retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

Article 5 of the GDPR provides that personal data shall be kept in a form which permits identification of subjects for no longer than is necessary for the purposes for which the personal data are processed. Specific time periods for retention of personal data are not stipulated by the GDPR or the Act. A controller must ensure that an appropriate time limit is established for the erasure of personal data and the carrying out of periodical reviews of the need for retention of the data.

Certain Irish legislation stipulates minimum retention periods for certain personal data, such as employee-related records.

13. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

Where a controller determines, by way of data protection impact assessment ("**DPIA**") that the intended processing would result in a high risk to the data protection rights of individuals in the absence of mitigation measures they must consult with the DPC.

14. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?

The legislative requirements have been interpreted as requiring organisations to carry out risk assessments in relation to all data processing activities. More specifically, where controllers or processors are processing personal data that is likely to result in a high risk to the data subject's rights, a DPIA must be carried out prior to commencing that processing. The GDPR provides some non-exhaustive examples of when data processing is likely to result in high risks. High risk processing includes large scale processing of special categories of personal data, or processing of personal data relating to criminal convictions and offences. The DPC has adopted "List of Types of Data Processing Operations which require a DPIA".

Risk assessments are also required in relation to transfers outside the EEA not subject to an adequacy decision.

15. Do the laws in your jurisdiction require appointment of a data protection officer (or other person to be in charge of privacy or data protection at the organization) and what are their legal responsibilities?

An organisation is required to appoint a designated DPO, where the processing is carried out by a public authority or body; the core activities require regular and systematic monitoring of data subjects on a large scale; or the core activities consist of processing on a large scale of special category data or data relating to criminal convictions and offences. The duties of DPOs include advising the organisation on data protection obligations, monitoring compliance including audits and training, acting as a contact point for the DPC and handling queries or complaints.

16. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

One of the legislative duties of the DPO is to oversee the training of staff by the organisation. The DPC advises that it is good practice to provide all staff with data protection training on or shortly after commencing employment. Evidence of ongoing training is considered necessary to demonstrate compliance with the principle of accountability and to ensure compliance with other provisions of the GDPR.

17. Do the laws in your jurisdiction require businesses to providing notice to individuals of their processing activities? If so, please describe these notice requirements (e.g., posting an online privacy notice).

The principle of transparency set out in the GDPR requires controllers to provide information to individuals about how their data is processed. The minimum required information to be provided to data subjects includes the identity of the controller/data processor, the reason for processing the data, the lawful basis for processing the personal data, applicable data transfer details, data retention timeframe and the existence of the individual's rights under data protection law. The information above is typically provided by way of a data privacy notice on the controller's website.

Pursuant to the e-Privacy Regulations, subscribers must be informed of the types of data that are processed, the

duration of such processing, the possibility to withdraw their consent and whether the data will be transmitted to a third party for specified purposes.

18. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data and, if so, what are they? (e.g., are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

The GDPR imposes obligations on both controllers and data processors. However, a clear distinction is drawn between controllers and processors. Primary responsibility for the protection of personal data under the GDPR is placed on controllers. A processor will be liable only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

19. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

Article 28(3) of the GDPR imposes an obligation on controllers and processors to enter into a legally binding contract, known as a data processing agreement ("**DPA**"), when a controller engages a processor to process personal data on its behalf. The DPA sets out certain mandatory terms, which must be included. Article 28 also requires a controller to carry out due diligence in relation to a processor prior to their appointment.

20. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction including the use of tracking technologies such as cookies. How are these terms defined and what restrictions are imposed, if any?

Monitoring is not specifically restricted or prohibited by the GDPR or the Act. However, a controller must establish a lawful basis for processing, and large scale monitoring of a publically accessible area requires completion of a DPIA.

Automated decision making (including profiling) is prohibited, where it produces legal effects concerning an individual. There are some exceptions to this prohibition for example; where the decision is authorised or required under Irish law (e.g. Section 851(b) (3) of the Taxes Consolidation Act 1997, as amended).

The e-Privacy Regulations prohibit the use of cookies which are not strictly necessary unless the subscriber or user has given his or her explicit consent to that use. The method by which such consent can be given has evolved in light of the GDPR and the Court of Justice of the European Union ("**CJEU**") case law. Consent for the placement of cookies is not valid if it is obtained by way of pre-checked boxes which users must deselect to refuse their consent. Controllers must ensure that opt in consent is obtained for each purpose for which cookies are set.

21. Please describe any restrictions on cross-contextual behavioral advertising. How is this term or related terms defined?

Cross-contextual behavioural advertising is not defined in Irish data protection legislation. The rules as outlined in the e-Privacy Regulations, the Act and the GDPR are therefore directly applicable to any form of cross-contextual behavioural advertising. This form of processing must have a lawful basis. The DPC has published a draft decision DPC Case Reference: IN-18-5-5 where it states that, in principle, an organisation could rely on the legal basis of contractual necessity for the processing required to deliver behavioural advertising insofar as this formed a core part of the service offered to and accepted by users and under the contract between the parties.

The Advertising Standard Authority of Ireland ("**ASAI**") is an independent, self-regulatory body which promotes high standards of marketing communications in Ireland. The ASAI has published rules on online behavioural advertising as part of its advertising code. However, this Code does not have legally binding force.

22. Please describe any laws in your jurisdiction addressing the sale of personal information. How is "sale" or related terms defined and what restrictions are imposed, if any?

"Sale" in the context of sale of personal information is not defined in Irish law, however is captured by the

broad definition of processing. Therefore, a controller must comply with all of the legal obligations applicable to the processing of personal data under the GDPR, including the core principles as outlined in response to question 4 above.

23. Please describe any laws in your jurisdiction addressing telephone calls, text messaging, email communication or direct marketing. How are these terms defined and what restrictions are imposed, if any?

Direct marketing is governed by both the GDPR and the e-Privacy Regulations. The e-Privacy Regulations prohibit unsolicited communication such as the use of electronic mail for direct marketing purposes without prior consent of a subscriber or user (except in certain circumstances relating to existing customers). The e-Privacy Regulations provide that individuals have the right to object to receiving electronic direct marketing and that a facility to opt-out must be included with each marketing communication.

24. Please describe any laws in your jurisdiction addressing biometrics, such as facial recognition. How are these terms defined and what restrictions are imposed, if any?

The processing of biometric data is prohibited except in certain circumstances as set out in Article 9 of the GDPR. The processing of biometric data is considered to be a high risk activity that requires a DPIA to be conducted. The DPC has also advised that the processing of biometric data should generally be optional for the user.

25. Is the transfer of personal data or PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

Transfers of personal data from Ireland to non-EEA or 'third' countries are governed by Chapter V of the GDPR. Such transfers are permitted either where there is an EU Commission adequacy decision in place or, alternatively, where appropriate safeguards are implemented, such as standard contractual clauses ("**SCCs**") or binding corporate rules under Article 46 of the GDPR. Derogations may also apply in limited circumstances under Article 49 of the GDPR.

Where SCCs are used, they must comply with the European Data Protection Board ("**EDPB**") recommendations[1] on measures to support the implementation of *Schrems II*.[2] In particular, the exporter must carry out a transfer risk assessment and also identify and implement supplementary measures to ensure an "essentially equivalent" level of protection applies to the personal data throughout the transfer.

SCCs must be governed by the laws of one of the EU Member States which provides for third-party beneficiary rights. The European Union (Enforcement of data subjects' rights on transfer of personal data outside the European Union) Regulations 2021 amend the Act to provide for these third party beneficiary rights.

References

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Adopted on 18 June 2021.

[2] CJEU, Judgment of 16 July 2020, C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*.

26. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

Controllers and processors are obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from processing activities. The Act does not stipulate any specific security measures. The GDPR lists certain considerations that should be taken into account, such as the costs of implementation and the nature, scope, context and purposes of processing. The DPC has issued Guidance for Controllers on Data Security dated February 2020.

The e-Privacy regulations impose certain security obligations on undertakings providing a publically available electronic communications network or service. Security measures must at least ensure that the personal data can be accessed only by authorised personnel for legally authorised purposes, protect

personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and ensure the implementation of a security policy with respect to the processing of personal data.

27. Do the laws in your jurisdiction address security breaches and, if so, how does the law define "security breach"?

GDPR utilises the term 'personal data breach' defined in accordance with the GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 (the "**NIS Regulations**") use the term "incident" which is defined as any event having an actual adverse effect on the security of network and information systems.

28. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

Legislative security requirements exist in relation to certain sectors such as the payment services sector, digital service providers and operators of essential services, for example:

- The European Union (Payment Services) Regulations 2018 introduced strict rules relating to electronic payments (particularly online payments). Strong Customer Authentication must be used to confirm a customer's identity or confirm that the customers authorises the payment.
- The NIS Regulations apply to digital service providers and operators of essential services and requires these organisations to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems they use.

29. Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator and what is the typical custom or practice in your jurisdiction?

A controller is obliged to notify the DPC within 72 hours of becoming aware of a personal data breach, unless it is unlikely to result in a risk to individuals. Separately, controllers are also obliged to notify the affected data subject of the personal data breach, where the breach is 'likely to result in a high risk to the rights and freedoms of the natural person'.

The NIS Regulations require notification by digital service operators and operations of essential service of an incident to the National Cyber Security Centre ("**NCSC**") where the incident (as defined in question 27 above) has a substantial impact on the provision of a digital service or on the continuity of an essential service.

The Central Bank of Ireland ("**CBI**") *Cross Industry Guidance in respect of Information Technology and Cyber Security Risks* provides that the CBI expects that firms will notify it when the firm becomes aware of a cyber-security incident that could have a significant and adverse effect on a firm's ability to provide adequate services to its customers, its reputation or financial condition.

Section 19 of the Criminal Justice Act 2011 imposes a mandatory obligation to report certain cyber security offences, in certain circumstances, to the Irish police.

The European Communities (Electronic Communications) (Framework) Regulations 2011 require an operator (providing public communications network or publically available electronic communications) to notify the Commission for Communications Regulation in the event of a breach of security or loss of integrity that have a significant impact on the operation of networks or services.

30. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cyber-crime, such as the payment of ransoms in ransomware attacks?

Where cyber-crime impacts on personal data, there are legal obligations to report a breach to the DPC and to data subjects in some instances (as set out at question 29 above).

Outside of the context of data protection, there are limited laws and guidelines in relation to dealing with cyber-crime while there are obligations to notify (set out at question 29 above).

In a recent large scale cyber-attack on the state health agency the government's policy was not to pay the ransom.

31. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

There is no cybersecurity regulator in Ireland. The NCSC is the government's operational unit for network and information security. One of its roles includes the provision of guidance and advice to citizens and businesses on major cybersecurity incidents.

32. Do the laws in your jurisdiction provide individual data privacy rights, such as the right to access and the right to deletion? If so, please provide a general description of the rights, how they are exercised, what exceptions exist and any other relevant details.

In accordance with the GDPR, individuals have various rights including the right of access, right of erasure, right of rectification, right of restriction and right of data portability. Data subjects can exercise their rights by contacting the controller who must respond without undue delay and at the latest within one month of receipt of the request.

Please see response to question 9 with regard to the restriction of rights.

33. Are individual data privacy rights exercisable through the judicial system or enforced by a regulator or both?

Individual privacy rights are exercisable through both the judicial system and through enforcement by the DPC. The data subject is entitled to both bring a civil action and submit a complaint to the DPC.

34. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

Where a data subject considers that their rights have been infringed as a result of personal data processing they may bring a data protection action against the controller or processor concerned to the Circuit or High Court. While representative actions are permitted under Irish law, they are rarely used due to various limitations.

35. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data privacy laws? Is actual damage required or is injury of feelings sufficient?

Section 117 of the Act permits an individual to seek compensation for the damage suffered as a result of the infringement of data protection laws. Damage includes material and non-material damage. Case law in this area remains unsettled. There are currently a number of cases awaiting judgement before the CJEU, which will influence the approach taken by the Irish Courts.

36. How are the laws governing privacy and data protection enforced?

Privacy and data protection laws are enforced through the DPC and the Courts. The DPC possesses broad enforcement powers, as well as investigatory powers including search and seizure powers, power to issue information and enforcement notices for which failure to comply is an offence and a right to apply to the High Court for the suspension or restriction of processing of data, where it is considered that there is an urgent need to act. The DPC also has the power to prosecute offences under the Act and the e-Privacy Regulations.

37. What is the range of sanctions (including fines and penalties) for violation of these laws?

Regulatory fines for breaches of data protection law can be up to €20,000,000 or 4% of global annual turnover of the relevant organisation, depending on the nature of the infringement. Other sanctions include a temporary or permanent ban on the processing of personal data, a reprimand or withdrawal of certification.

The Act imposes a maximum fine of up to €1,000,000 on public authorities or bodies that do not act as an undertaking within the meaning of the Irish Competition Act 2002.

The maximum criminal penalty for summary offences under the Act is €5,000 and/or 12 months' imprisonment. Indictable offences and carry a maximum penalty of €250,000 and/or five years' imprisonment.

The DPC does not have the power to impose regulatory fines pursuant to the e-Privacy Regulations. However, offences under these regulations can be prosecuted in the Court. A summary offence carries a maximum fine of €5,000. Indictable offences carry a maximum fine of

€250,000 depending on the nature of the offence being prosecuted.

38. Are there any guidelines or rules published regarding the calculation of fines or thresholds for the imposition of sanctions?

The GDPR is silent as to the particular process or methodology which supervisory authorities such as the DPC should adopt in calculating a fine or sanction, however the DPC is required to consider certain factors as stipulated by Article 83 of the GDPR. The DPC has demonstrated an assessment of these factors in its published decisions. As a matter of domestic law, the DPC'S decision must be demonstrably rational and not arbitrary.

Fines or sanctions administered by the Court in the context of prosecutions are at the discretion of the judge.

39. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Under the Irish regime, controllers or processors can appeal fines imposed by the DPC, within 28 days of receipt of the decision.

Upon hearing an appeal, the Court may confirm the decision of the DPC, impose a different fine, or annul the decision of the DPC.

Where an organisation wishes to challenge the decision making process of the DPC they may do so by way of judicial review.

40. Are there any proposals for reforming data protection or cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

In a recent decision, the CJEU has concluded that the general and indiscriminate retention of electronic traffic and location data for law enforcement purposes is precluded by EU law. At the time of writing, proposed legislation namely the Communications (Data, Retention and Disclosure) Bill has been published and prioritised by the Irish Government. This proposed legislation is intended to revoke the 2011 e-Privacy Regulations in light of recent CJEU jurisprudence.

The European Commission has proposed a new Regulation on Privacy and Electronic Communications which, at the time of writing, remain under review by the Council of the European Union. This new Regulation will repeal the existing 2002 e-Privacy Directive and will have direct effect in Ireland once enacted.

The Irish Government has recently published the General Scheme of the Representative Actions for the Protection of the Collective Interest of Consumers Bill 2022. This legislation, once enacted, is likely to have a significant impact on the manner in which data protection actions in Ireland are litigated.

Contributors

Jon Legorburu
Partner and Head of Litigation and Dispute Resolution
jlegorburu@byrnewallace.com

Seán O'Donnell
Partner, Litigation and Dispute Resolution/Privacy & Data Protection
sodonnell@byrnewallace.com

Zelda Deasy
Partner, Corporate/Privacy & Data Protection
zdeasy@byrnewallace.com