COUNTRY COMPARATIVE GUIDES 2023

The Legal 500 Country Comparative Guides

Ireland

DATA PROTECTION & CYBERSECURITY

Contributor

ByrneWallace LLP

Jon Legorburu

Partner, Head of Cybersecurity and Head of Litigation & 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

Eimear Redmond

Solicitor, Litigation and Dispute Resolution/Privacy & Data Protection | eredmond@byrnewallace.com

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

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

IRELAND
DATA PROTECTION & CYBERSECURITY

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity 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).

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 into national law Directive (EU) 2016/680 ("**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 Data Protection Commission ("**DPC**") is the national competent authority for the regulation and enforcement this legislation.

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, as amended ("**e-Privacy Regulations**") transpose Directive 2002/58/EC "**e-Privacy Directive**"). 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 e-Privacy Regulations were amended by the European Union (Electronic Communications Code) Regulations 2022 which increased the range of service providers falling within the scope of the legislative requirements.

The Data Sharing and Governance Act 2019 ("**2019 Act**") regulates the sharing of information, including personal data, between public bodies, provides for the establishment of base registries and the Personal Data Access Portal, and established the Data Governance Board.

Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification ("**Cybersecurity Act**") has direct effect in Ireland and grants a cybersecurity certification and operational cooperation mandate to ENISA and introduces an EU-wide cybersecurity certification framework for ICT products, services and processes.

The European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018 ("**NIS Regulations**") transposes Directive (EU) 2016/114 and applies a set of binding security obligations to critical infrastructure operators in the energy, healthcare, financial services, transport, drinking water supply and digital infrastructure and telecommunications sectors. A unit of the Department of Communications, Climate Action and Environment, the Computer Security Incident Response Team ("**CSIRT**"), is designated as the computer security incident response team in the State. The Minister for the Environment, Climate and Communications ("**Minister**") is the designated competent authority for the purposes of enforcement against providers within all sectors as well as digital services providers, other than the banking and financial market infrastructure sectors to which the Central Bank of Ireland ("**CBI**") is designated. Ireland has responsibility for dealing with the security of services provided by multinational companies across the European Union that have their European headquarters located in Ireland.

The Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 gives effect to certain provisions of EU Directive 2018/1972 which established the European Electronic Communications Code. This Act mandates that providers of public electronic communications networks and services take appropriate and proportionate measures to manage the risks posed to the security of networks and services. This Act designates the Commission for

Communications Regulations (**"ComReg**") as the competent authority for the purposes of enforcement in the State. A substantive part of this Act is yet to be commenced. The European Union (Electronic Communications Code) Regulations 2022 transpose the remainder of the Directive.

2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

Irish law is expected to evolve considerably in light of significant developments to the EU legislative landscape.

Regulation (EU) 2022/868 on European data governance ("**Data Governance Act**") will apply in Ireland from September 2023.

Regulation (EU) 2022/2065 a Single Market For Digital Services (the "**Digital Services Act**" or "**DSA**") came into effect in November 2022 and Ireland must designate a 'Digital Services Co-Ordinator' ("**DSC**") by February 2024.

Regulation EU 2022/2554 on digital operational resilience for the financial sector ("**DORA**"), and Directive EU 2022/2556 ("**DORA Amending Directive**") will apply in Ireland from January 2025.

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("**NIS2 Directive**") and Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC ("**CER Directive**") are required to be transposed into Irish law by October 2024.

The European Commission has also proposed new legislation including the Regulation concerning the respect for private life and the protection of personal data in electronic communication ("**ePrivacy Regulation**"), the Regulation on harmonised rules on fair access to and use of data ("**Data Act**"); the Regulation on horizontal cybersecurity requirements for products with digital elements ("**Cyber Resilience Act**"); and the Regulation laying down harmonised rules on artificial intelligence ("**Artificial Intelligence Act**").

The Communications (Retention of Data) (Amendment) Act 2022, once commenced, will amend the e-Privacy Regulations and requires electronic communications service providers to retain data for one year or such a time period as may be prescribed by the Minister for Justice for the purposes of preventing, detecting, investigating or prosecuting offences, safeguarding the security of the State, protecting personal safety and the search for missing persons.

Furthermore, the Irish Government's Spring Legislative Programme 2023 includes the following draft legislation currently subject to legislative scrutiny:

i. The Representative Actions for the Protection of the Collective Interest of Consumers Bill applies to domestic and cross-border infringements of certain legislation, including the Data Protection Act 2018. Once enacted, it will enable consumers to be represented collectively by non-profit "qualified entities";
ii. The Health Information Bill will provide for the appointment of a National Health Information Guardian who will oversee the use of health data and the establishment of a National Health Information Centre that will govern the procedures for collecting data for population health and research purposes;
iii. The Cyber Security Bill will establish the National Cyber Security Centre ("**NCSC**") on a statutory basis and provide for related matters including clarity around its mandate and role;
iv. The aim of the Communications (Data, Retention and Disclosure) Bill is to consolidate and replace the current Communications (Retention of Data) Act 2011; and
v. The aim of Criminal Justice (Passenger Name Record) Bill is to comply with an EU Council commitment to extend to internal EU flights the requirements of EU Directive 2016/681 on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

3. 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. Competent authority under the NIS Regulations are required to establish and maintain a Register of Operators of Essential Services. There are no specific

exemptions stipulated by the NIS Regulations.

4. 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?

Irish law adopts the definitions of personal data and special category data in accordance with the GDPR. 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.

5. 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.

Irish law requires that data must be processed in accordance with the principles in Article 5 GDPR. 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.

6. 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) Regulations, as amended.

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 required for the use of non-necessary cookies (see response 22). Consent is often the most appropriate basis for the use of biometric data. See response 26.

7. 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, inactivity and other forms of implied consent 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.

8. 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 or disclosure?

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. Criminal offence data is also offered special protection and can only be processed in certain limited circumstances. Different restrictions apply where the data is processed for law enforcement purposes.

9. How do the laws in your jurisdiction address children's personal data?

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 introduced child-specific data protection interpretative principles and recommended measures to enhance the level of protection afforded to children. The digital age of consent in Ireland is 16 years, 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 years, 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. See response 23.

10. How do the laws in your jurisdiction address health data?

In addition to the protections under GDPR and the Act, the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018, as amended, set out stringent rules governing the collection, use and sharing of personal data for health research purposes. There is also specific legislation which allows for the collection and processing of specific personal health data in Ireland; for example, the Infectious Disease Regulation, 1981, National Cancer Registry Board (Establishment) Order, 1991, and the Statistics Act, 1993.

11. Do the laws 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 and 94 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 rules applicable to the transfer of data outside the EEA.

12. 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 and section 76 of the Act. 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.

13. Are owners/controllers 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 (a "**ROPA**"). The ROPA must be in writing, including electronic form and must be updated regularly and available for submission to the DPC upon request. Companies or institutions with fewer than 250 employees are exempt from keeping a record in certain circumstances, although a ROPA is mandatory for all organisations for HR data.

14. 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 data 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 that data.

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

15. 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.

16. 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. 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 a "List of Types of Data Processing Operations which require a DPIA".

Risk assessments are also required in relation to transfers outside the EEA that are not subject to a European Commission adequacy decision, to ensure that the country provides an equivalent level of protection to personal data as provided by the GDPR.

17. Do the laws in your jurisdiction require appointment of a data protection officer or a chief information security 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. Article 27 of the GDPR requires non-EU organisations to designate in writing a representative in the EU unless one of the specified exemptions applies.

18. 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.

19. Do the laws in your jurisdiction require businesses to provide notice to data subjects 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.

20. 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? (For example, 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 processors. However, a clear distinction is drawn: 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 the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

21. 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. Article 28 prescribes 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.

22. 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.

The e-Privacy Regulations prohibit the use of cookies or other tracking technologies which are not strictly necessary unless the user has given explicit consent to that use. The standard of consent is set out under the GDPR. Consent for the placement of non-essential cookies is not valid if it was either bundled or obtained by way of pre-checked boxes that users must deselect. Controllers must ensure that opt-in consent is obtained for each purpose for which cookies are set and consent must be as easy to withdraw as it was to provide in the first place.

23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms 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.

Targeted advertising is a form of data processing that must have a lawful basis, which is usually consent. In a joint decision adopted in January 2023 the DPC, as instructed by the EDPB, imposed a €390 million fine on Meta on the basis that Meta was not entitled to rely on contractual necessity as the lawful basis to process personal data for the purpose of behavioural advertising because, crucially, this was not a core element of the services.

The DSA prescribes transparency rules and prohibits the use of certain data types (including special category data) for targeted advertising for online platforms. The DSA prohibits targeted advertising aimed at children and requires service providers to carry out a risk assessment of the risk that their platform may pose to children. The General Scheme of the Digital Services Bill was published in February 2023 and will give effect to the DSA.

24. Please describe any laws in your jurisdiction addressing the sale of personal data. 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 5 above.

25. 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). Individuals have the right to withdraw consent or object to receiving electronic direct marketing. A facility to opt-out must be included with each marketing communication.

26. 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.

Amendments to the Garda Síochána (Recording Devices) Bill 2022, namely to permit the use of facial recognition technology to be worn by An Garda Síochána (Irish police), have been proposed however this is subject to intense debate and it remains to be seen whether such amendments will be adopted.

27. 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 e.g. where a data subject explicitly consents. In June 2021, the European Commission approved four separate modular sets of SCCs and the appropriate module to be used will depend on the data protection role of the data exporter and data importer. Where SCCs are used, they should comply with the European Data Protection Board recommendations (Recommendations 01/2020) on measures to support the implementation of the decision in C-*311/18 Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems.* 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 to the third country.

28. 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. Neither the GDPR nor the Act 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.

29. Do the data protection, privacy and cybersecurity 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 NIS Regulations define the term "incident" as any event having an actual adverse effect on the security of network and information systems.

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

In addition to the legislation as specified above, the European Union (Payment Services) Regulations 2018 applies strict rules relating to electronic payments (particularly online payments).

31. 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. 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 competent authority (the CSIRT or the CBI as the case may be) where the incident (as defined in question 29 above) has a substantial impact on the provision of a digital service or on the continuity of an essential service.

The 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 cybersecurity 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 cybersecurity offences, in certain circumstances, to the Irish police.

Providers of public electronic communications networks and services must notify users of a significant threat of a security incident pursuant to the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023. Providers of are required to notify ComReg, of any security incident that will have a significant impact on the provider's networks or services pursuant to this Act as well as the E-Privacy Regulations.

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

Outside of the context of notification obligations under GDPR, the Act or the NIS Regulations, there are limited laws and guidelines in relation to dealing with cyber-crime (see response 31). The NCSC published Guidance in August 2022 on compliance by operators of essential services with the NIS Regulations. We understand that the position of the NCSC is that ransoms should not be paid.

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

There is no cybersecurity regulator in Ireland. The NCSC is the Irish 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. The Minister and the CBI are designated competent authorities pursuant to the NIS Regulations.

34. 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 (this time period can be extended by up to two months in exceptional circumstances). See response 11 with regard to the restriction of rights.

35. 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.

36. 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.

37. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection, privacy and/or cybersecurity 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. The Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 provide for end-user compensation where there is a failure by a provider of internet access services or number-based interpersonal communications service.

38. How are data protection, privacy and cybersecurity laws 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.

The DSA will be enforced by the European Commission and Member States DSCs in respect of intermediary services with their main establishment in that Member State. The Digital Services Bill is currently being progressed to designate Comisiún na Meán as the DSC and invest it with the necessary powers to carry out its functions under the DSA. The DSCs have wide powers of investigation and powers to impose administrative sanctions.

The NIS Regulations are enforced by the Minister or the Central Bank of Ireland, depending on the relevant sector. The competent authority may issue compliance notices which may be appealed to the Circuit Court. Failure to comply with a compliance notice which has not been cancelled by the Circuit Court is a criminal offence.

ComReg is empowered to issue administrative sanctions in response to infringements of Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023.

39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

Regulatory fines for breaches of data protection law can be up to the greater of €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.

In the event of non-compliance with the DSA, service providers could receive a fine of up to 6% of their annual global turnover.

A person guilty of an offence under the NIS Regulations is liable on summary conviction to a fine not exceeding €5,000. Indictable offences carry a maximum penalty of €50,000 in the case of an individual and €500,000 in the case of a body corporate.

Where an adjudicator deems that a breach has been committed under the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023, they may issue a fine of up to €5,000,000 or 10% of turnover for a corporate body or up to €500,000 or 10% of the annual income of a natural person. This fine must be confirmed by the High Court.

40. 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 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. In May 2022 the EDPB published Guidelines on the calculation of administrative fines under the GDPR (Guidelines 04/2022). 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.

The Digital Services Bill provides that Coimisiún na Meán, in setting the fine in any particular case, must take into account a number of factors, as listed within the Broadcasting Act, as amended by the Online Safety and Media Regulation Act 2022.

An adjudicator must have regard to guidelines published by ComReg in respect of the imposition of a financial sanction pursuant to the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023.

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

42. Are there any identifiable trends in enforcement activity in your jurisdiction?

In 2022 the DPC imposed administrative fines in excess of €1 billion which represented two-thirds of the fines issued in the EU, EEA, and UK. This reflects the DPC's reputation as an active enforcement body, a consequence of the "one-stop-shop mechanism" whereby the DPC is designated as the lead supervisory authority for organisations with their main establishment in Ireland. In the 2022 DPC Annual Report the Commissioner described this mechanism as a "legal maze that requires constant navigation". In the Regulatory Strategy 2022-2027, the DPC commits to seek clarification and consistency on procedures under the One-Stop-Shop mechanism and international cooperation. The number of breaches notified under the e-Privacy Regulations represented a three-fold increase on 2022, due to amendments to the e-Privacy Regulations aforementioned.

2023 commenced with significant fines for large social media platforms. Recent decisions have highlighted tensions between the DPC, its European counterparts and the EDPB vis-à-vis enforcement in particular, the differences of opinion that can arise in relation to the appropriate level of administrative fines to be awarded against such companies. Although media attention is focused on enforcement against 'big tech', there is evidence of the DPC enforcing data protection and direct marketing laws across all sectors. The DPC has also sought sanction from the Irish Government for additional resources. In July 2022 the Irish Government announced the appointment of two additional Commissioners. This will assist with the administrative burden to which the DPC is currently subject and is expected to expedite enforcement.

43. Are there any proposals for reforming data protection, privacy and/or

cybersecurity laws currently under review? Please provide an overview of any proposed changes and how far such proposals are through the legislative process.

Please see response to question 2. The National Cyber Security Strategy, published in 2019, is aimed at enhancing the security and resilience of Government systems and critical national infrastructure. This strategy is currently subject to a mid-term review consultation in recognition of the changed global cyber threat landscape and evolution of the EU legislative framework.

Contributors

Jon Legorburu
Partner, Head of Cybersecurity and Head of Litigation & 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

Eimear Redmond
Solicitor, Litigation and Dispute Resolution/Privacy & Data Protection
eredmond@byrnewallace.com