COUNTRY COMPARATIVE GUIDES 2024

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

Alan Grace

Privacy Counsel, Litigation and Dispute Resolution/Privacy & Data Protection | algrace@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 ("**2018 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 to 2003 as amended also still apply in certain limited circumstances.

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

The Data Sharing and Governance Act 2019, as amended ("**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, in addition to introducing 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, water supply, 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 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 with European headquarters in Ireland.

The Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023 (as amended) gives effect to certain provisions of EU Directive 2018/1972, which established the European Electronic Communications Code and was fully commenced on 9 June 2023. 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 Regulation (**"ComReg**") as the competent authority for the

purposes of enforcement in the State. The European Union (Electronic Communications Code) Regulations 2022 transpose the remainder of the Directive.

The Digital Services Act 2024 was enacted on 17 February 2024, giving further effect to Regulation (EU) 2022/2065 on a Single Market for Digital Services which empowers the European Commission to regulate online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. It aims to prevent illegal and harmful activities online and the spread of disinformation.

The Policing, Security and Community Safety Act 2024, was signed into law on 7 February 2024, and empowers the Garda Síochána, the Authority (*An tÚdarás Póilíneachta agus Sábháilteachta Pobail)*, or the Police Ombudsman to share data with other agencies to perform its functions, and amends the Communication Act 2011.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

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

Regulation (EU) 2022/2065 on a Single Market for Digital Services (the "**DSA**") came into effect in November 2022 and Ireland designated Comisiúin na Meán ("**CNM"**) as the 'Digital Services Co-Ordinator' ("**DSC**") for this jurisdiction. Additionally, the DSA designates the Competition and Consumer Protection Commission as the competent authority for dealing with traceability of traders, compliance by design and right to information requests.

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 a new Regulation concerning the respect for private life and the protection of personal data in electronic communication ("**ePrivacy Regulation**"). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) entered into force on 11 January 2024; the Regulation on horizontal cybersecurity requirements for products with digital elements ("**Cyber Resilience Act**") had its text agreed in December 2023; and the Regulation laying down harmonised rules on artificial intelligence ("**AI Act**") has been agreed by the Council, and the text of the Act is in the Process of being formally adopted and translated. The AI Act will enter into force 20 days after its publication in the Official Journal, and will be fully applicable 2 years later.

The Communications (Retention of Data) (Amendment) Act 2022, fully commenced in July 2023, amends the e-Privacy Regulations and requires electronic communications service providers to retain data for one year or such 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 or protecting personal safety and the search for missing persons.

In the last year, the following Bills have been progressed by the Government:

i. The Representative Actions for the Protection of the Collective Interest of Consumers Act was signed into law on 11 July 2023, but is yet to be commenced by the Minister. The Act applies to domestic and cross-border infringements of certain legislation, including the 2018 Act. Once enacted, it will enable consumers to be represented collectively by non-profit "qualified entities";
ii. The Health Information Bill's general scheme was approved by the Government on 18 April 2023, and 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; and
iii. Work has begun on the preparation of a general scheme to the Cyber Security Bill with a view to meeting a transposition deadline of 17th October 2024. The 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.

3. Are there any registration or licensing requirements for entities covered by these data protection 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. A competent authority is required under the NIS Regulations to establish and maintain a Register of Operators of Essential Services ("**ROES**") without exception.

4. How do these data protection laws define "personal data," "personal information," "personally identifiable information" or any equivalent term in such legislation (collectively, "personal data") versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

Irish law adopts the definitions of personal data and special category data in accordance with the GDPR. The 2018 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. 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 in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

Article 5 of the GDPR sets out key principles for the protection of personal data. These principles both directly and indirectly influence the other rules and obligations found throughout the applicable legislation. Compliance with these fundamental principles of data protection is the first step for controllers in ensuring that they fulfil their obligations under the GDPR. The following is a brief overview of the Article 5 principles:

Lawfulness, fairness, and transparency: Any processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.

Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In particular, the specific purposes for which personal data are processed should be explicit, legitimate and determined at the time of the collection of the personal data. However, further processing for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes (in accordance with Article 89(1) GDPR) is not considered to be incompatible with the initial purposes.

Data Minimisation: Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum (see also the principle of 'Storage Limitation' below).

Accuracy: Controllers must ensure that personal data are accurate and, where necessary, kept up to date; taking every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. In particular, controllers should accurately record information they collect or receive and the source of that information.

Storage Limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to, or

use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability: The controller is responsible for, and must be able to demonstrate compliance with all of the above principles. Controllers must take responsibility for their processing of personal data and how they comply with the GDPR, and be able to demonstrate (through appropriate records and measures) their compliance, in particular to the DPC.

In addition, the processing must be established on one of the six legal bases for processing provided by Article 6 of the GDPR. Article 6 of the GDPR sets out what these potential legal bases are, namely: consent; contract; legal obligation; vital interests; public task; or legitimate interests.

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited, unless one of the conditions set out in Article 9(2) of the GDPR applies.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

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

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.

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, such as in the context of an employer/employee relationship.

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 personal data? Are any categories of personal data prohibited from collection or disclosure?

The GDPR provides extra protection for certain categories of personal data, called "special category data", under Article 9 of the GDPR. Special category data refers to data which reveals:

"*Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*".

These categories of personal data shall not be processed unless a controller can avail of one of the exceptions under Article 9(2) of the GDPR. These exceptions include explicit consent, exceptions on the basis of employment or social protection law and processing in respect of the courts acting in their judicial capacity.

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 data protection laws in your jurisdiction address health data?

In addition to the protections under the GDPR and the 2018 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 as amended, National Cancer Registry Board (Establishment) Order, 1991, and the Statistics Act, 1993.

10. Do the data protection laws in your jurisdiction include any derogations, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

The GDPR and the 2018 Act set out various derogations, exclusions and limitations, for example in relation to data subject rights. Article 23 GDPR creates the right for Member States to introduce derogations to data protection law in certain situations. Member States can introduce derogations from transparency obligations and data subject rights, but only where the measure "respects the essence of fundamental rights and freedoms and is necessary and proportionate in a democratic society".

In addition to this, the provisions in Chapter IX of the GDPR provide for a mixed set of derogations, exemptions and powers to impose additional requirements, in respect of GDPR obligations and rights, for particular types of processing.

The 2018 Act permits controllers to restrict data subject rights where it is necessary and proportionate to safeguard certain objectives, as set out in Sections 60 and 94 of the 2018 Act. Examples of such restrictions include:

1. Data Protection Act 2018 (section 60(6)) (Central Bank of Ireland) Regulations 2020 restricts data subject access to information for which the CBI is the controller in certain circumstances.
2. 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.

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

The GDPR and the 2018 Act apply to children and adults equally. Under Section 29 of the 2018 Act, a child is defined as a person under the age of 18 years. Sections 30 to 33 of the 2018 Act relate specifically to children and relate to the micro-targeting and profiling of children, the consent of a child in relation to information society services, codes of conduct in relation to children and a child's right to be forgotten. Section 30, which relates to the micro-targeting and profiling of children has not yet been commenced.

The age of digital consent in Ireland has been specified as 16 and online providers must make "reasonable efforts" to verify that a person with parental responsibility has consented to the processing of a child under the age of 16's personal data on their behalf, where consent is the legal basis relied upon for that processing.

The DSA was signed into law in Ireland in February 2024 and there is a strong focus in the DSA on better protection for children from online harm.

The Online Safety and Media Regulation Act, 2022 (the **"2022 Act**") was largely enacted in December 2022 and aims to regulate the provision of content though non-traditional media ranging from social media to online gaming. The 2022 Act aims regulate harmful content and create a safer online environment, in particular by addressing the causes of cyber bullying, self-harm or suicide, and material that promotes nutritional deprivation. The 2022 Act also provides for the establishment of CNM, whose remit includes the implementation of a new regulatory framework as well as holding designated online services to account through legally binding online safety codes.

In December 2021, the DPC published Fundamentals for a child-orientated approach to data processing, which introduced child-specific data protection interpretative principles and recommended measures to enhance the level of protection afforded to children when processing their personal data.

12. Do the data protection laws in your

jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The Harassment, Harmful Communications and Related Offences Act, 2020, also known as "Coco's Law", contains specific criminal offences that are applicable to online communications, such as taking or sharing intimate images of a person without their consent. According to An Garda Síochána, approximately 350 prosecutions have been commenced since the enactment of this law.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

Privacy and data protection laws are enforced in Ireland, in general, through the DPC and through the Courts. The DPC has broad enforcement and investigatory powers.

In addition to the DPC, in March 2023, CNM became the new media regulator for online safety, television broadcasting and video-on-demand services and, like the DPC, has broad enforcement and investigative powers. CNM, in accordance with its obligations under the 2022 Act, is currently developing Ireland's online safety code, part of which, will focus on illegal content which is harmful to children. The code will set out obligations in relation to how online services tackle the availability of harmful online content.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

There are no bills currently passing through the Irish system that relate directly to online safety.

Certain provisions of the 2022 Act are yet to be commenced.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

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 2018 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.

16. Are controllers and/or processors of personal data required to maintain any internal records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

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.

17. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

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 2018 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.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

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. In addition to this, the Controller has an obligation under the GDPR to notify the DPC within 72 hours once becoming aware of a personal data breach.

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under 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 data processing activities on an extensive basis. 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 commencement. 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 published guidance in this area to assist organisations in determining when a DPIA is required.

Risk assessments are also required in relation to transfers of personal data outside the EEA (including remote access) 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 or where this is not the case that supplementary measures are put in place to protect the data.

In addition, where the legitimate interests ground is relied on under Article 6(1)(f) of the GDPR as a lawful basis for processing, it is recommended best practice for the controller to carry out a Legitimate Interests Assessment ("**LIA**") which involves assessing the impact of the proposed processing on individuals' interests through a balancing test.

Organisations will differ in how risk assessments are carried out and much will depend on the organisation's risk assessment policy. It is important that the organisation's DPO is involved in such assessments.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, 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 of data subjects. 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.

21. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s).

One of the legislative duties of the DPO is to oversee 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.

22. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (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.

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.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

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.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

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, when a controller engages a processor to process personal data on its behalf. The areas that are required to be addressed in the contract are set out in Article 28 GDPR.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

Article 28 prescribes certain mandatory terms, which must be included, and also requires a controller to carry out due diligence in relation to a processor prior to their appointment.

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

Monitoring is not specifically restricted or prohibited by the GDPR or the 2018 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.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

Cross-contextual behavioural advertising is not defined in Irish data protection legislation. The rules as outlined in the e-Privacy Regulations 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.

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.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such 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.

29. Please describe any data protection 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.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such 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 carried out. The DPC has also advised that the processing of biometric data should generally be optional for the user.

An Garda Síochána (Recording Devices) Act 2023 was adopted on 5 December 2023, to permit the use of body-worn cameras by An Garda Síochána. Body-worn cameras are expected to be available to Dublin city centre Gardaí in the first half of 2024.

More controversial legislation is being taken forward by the government to allow An Garda Síochána to combine these bodycams with facial recognition technology.

31. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

The EU AI Act (the "**AI Act**") was approved by the European Parliament in March 2024, will come into effect 20 days after its publication in the Official Journal, and will be fully applicable two years after its entry into force, save for certain exceptions such as bans on prohibited practices, which will apply six months after the entry into force date; codes of practice (nine months after entry into force), general-purpose AI rules including governance (12 months after entry into force); and obligations for high-risk systems (36 months after entry into force).

The AI Act will follow a risk-based approach, differentiating between uses of AI that create an unacceptable risk, a high risk, and a low or minimal risk. The AI Act introduces EU-wide minimum requirements for AI systems and proposes a sliding scale of rules based on the risk: the higher the perceived risk, the stricter the rules. AI systems with an 'unacceptable level of risk' will be strictly prohibited and those considered as 'high-risk' will be permitted, but subject to very stringent obligations.

In terms of extra-territorial effect, the AI Act applies to providers placing on the market or putting into service AI systems in the EU, irrespective of whether those providers are established within the EU or a third country, users of AI systems located within the EU and providers and users of AI systems that are located in a third country, where the output produced by the system is in the EU.

AI systems are subject to the GDPR where personal data is added to AI or AI is otherwise used to process personal data.

The fines and penalties which may be imposed under the AI Act are significant and surpass those under the GDPR: Tier 1 fines for non-compliance with the prohibitions are up to €35,000,000 or up to 7% of annual worldwide turnover. Tier 2 fines for non-compliance with specific provisions are up to €15,000,000 or up to 3% of annual worldwide turnover. Tier 3 fines for supplying incorrect, incomplete or misleading information to the authorities is up to €7,500,000 or 1% of annual worldwide turnover.

32. Is the transfer of personal data outside your 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 or 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 ("**BCRs**"), under Article 46 of the GDPR. Derogations may also apply in limited circumstances under Article 49 of the GDPR. 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. In particular, the exporter must carry out a transfer risk assessment and also identify and implement supplementary measures, where required, to ensure an "essentially equivalent" level of protection applies to the personal data throughout the transfer to the third country.

33. What security obligations are imposed on data controllers and 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 2018 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 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.

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

The term 'personal data breach' is defined in 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.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

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

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard 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 it is expected firms will notify the CBI when

they become 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 Gardaí.

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 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.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Outside of the context of notification obligations under GDPR, the 2018 Act or the NIS Regulations, there are limited laws and guidelines in relation to dealing with cyber-crime. 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.

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

The NCSC was founded in 2011 and is an operational arm of the Department of the Environment, Climate and Communications ("**DECC**"). The NCSC is responsible for advising and informing Government IT and Critical National Infrastructure providers of current threats and vulnerabilities associated with network information security.

The main roles of the NCSC are to lead in the management of major cyber security incidents across government, provide guidance and advice to citizens and businesses on major cyber security incidents, and develop strong international relationships in the global cyber security community for the purposes of information sharing. In the period since 2011, the unit has focused its efforts on building capacity and establishing a stable base for its operational work.

The NCSC encompasses the State's National/Governmental Computer Security Incident Response Team (CSIRT-IE). CSIRT-IE is an internationally accredited response team with its main function being the enhancement of situational awareness for constituents and for the provision of incident response for national cyber security incidents. CSIRT-IE has initially focused on the State sector and acts as a national point of contact for all cyber security matters concerning Ireland.

39. Do the data protection 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 such rights, how they are exercised, any exceptions 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, right of data portability and right to make a complaint to the DPC. 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).

40. Are individual data privacy rights exercisable through the judicial system, 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.

41. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under 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 District, Circuit or High Court depending on the value of the claim. The Courts and Civil Law (Miscellaneous Provisions) Act 2023 added the District Court to the choices of venues for data protection litigation, the monetary average compensation for data breach claims is very modest and

well within the District Court level. However, the 2018 Act granted jurisdiction to the Circuit Court and High Court only. This resulted in costs of these claims exceeding their value. This new provision should mean these claims will now more properly be brought in the District Court.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is injury to feelings, emotional distress or similar sufficient for such purposes?

Section 117 of the 2018 Act permits an individual to seek compensation for damage caused 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 provides for end-user compensation where there is a failure by a provider of internet access services or number-based interpersonal communications service.

43. How are data protection laws in your jurisdiction 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 2018 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 DSA designates CNM as the DSC in Ireland. The DSCs have wide powers of investigation and powers to impose administrative sanctions.

The NIS Regulations are enforced by the Minister or the CBI, 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.

44. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

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 2018 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 2018 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, which must be confirmed by the High Court.

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

The GDPR is silent as to the process 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 DSA provides that CNM, in setting the fine in any particular case, must take into account a number of factors, as listed within the Broadcasting Act 2009, as amended by the 2022 Act.

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.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

In Ireland, 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.

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

In May 2023, Ireland continued its trend of applying significant fines on "big tech" companies when a fine of €1.2bn was imposed against Meta for the unlawful transfer and storage of personal data outside of the EEA.

A significant development occurred in January 2024 whereby jurisdiction was extended to the District Court to hear data protection actions, when Section 117 of the 2018 Act amended Section 77 of the Courts and Civil (Miscellaneous Provisions) Act 2023, extending the District Court's jurisdiction.

This extension will reduce costs associated with making a claim for a personal data breach and will likely apply to a significant amount of claims for non-material damage.

This extension is a welcome development for data controllers from a legal costs perspective. Many claims for non-material damages under Section 117 of the 2018 Act will now fall within the jurisdiction of the District Court.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

In addition to the legislative developments mentioned above, the Irish Government's Spring and Summer Legislative Programmes for 2024 include the following draft legislation currently subject to legislative scrutiny:

i. The Communications (Data, Retention and Disclosure) Bill which aims to consolidate and replace the current Communications (Retention of Data) Act 2011;
ii. The Criminal Justice (Passenger Name Record) Bill the purpose of which 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; and
iii. The Criminal Justice (Protection, Preservation and Access to Data on Information Systems) Bill 2024, which will allow law enforcement to request the preservation and production of data being held by internet service providers. The general scheme of the Bill was approved on 7 February 2024 and has been referred for pre-legislative scrutiny. The proposed legislation will give effect to the Council of Europe Budapest Convention on Cybercrime, the EU E-evidence Regulation (EU) 2023/1543 and the EU Terrorist Content Online Regulation (EU) 2021/784.

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

Alan Grace
Privacy Counsel, Litigation and Dispute Resolution/Privacy & Data Protection
algrace@byrnewallace.com

