Global Data and Cyber Handbook - Ireland

Security Requirements and Breach Notification

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 13 January 2025*

Yes.

☒  general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

☒  obligation to take specific security measures e.g., encryption

Not a strict legal requirement, but encryption is considered by the GDPR as an appropriate technical and organizational measure. In practice, the authorities expect encryption unless specific circumstances justify no encryption.

☒  other

In addition, the Protected Disclosures (Amendment) Act 2022 requires data controllers to implement controls and measures to ensure the security of personal data obtained during the whistleblowing process. This includes implementing secure storage and restricting access to the data, and ensuring the reporter's identity is not disclosed either accidentally or illegally. It also calls for technical and organizational provisions such as limiting access to the data to a limited number of designated individuals, and applying encryption, anonymization or pseudonymization.

# Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 13 January 2025*

☒       network information security requirements (broader than telecommunications)

☒       financial services requirements

☒       providers of critical infrastructure

☒       digital or connected (IoT) products

# Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

☒      Data privacy

The DPC concluded a number of inquiries over the last 12 months which considered whether the subject of the investigation had, among other considerations, complied with obligations under the GDPR to implement appropriate technical measures (including cybersecurity measures) to ensure an appropriate level of security for personal data being processed.

☒       other

The NCSC issued guidance on:

[Guidelines on Cybersecurity for Political Organisations and Election Candidates](https://www.ncsc.gov.ie/pdfs/NCSC_Cyber_Security_Political_Orgs_Candidates.pdf)

[National Cyber Emergency Plan](https://www.ncsc.gov.ie/pdfs/National_Cyber_Emergency_Plan.pdf)

[Guidance on Denial of Service Attacks](https://www.ncsc.gov.ie/pdfs/NCSC_DoS_Guidance.pdf)

[General Election 2024 Cyber Threat Landscape](https://www.ncsc.gov.ie/pdfs/Election_Cyber_Threat_Landscape2024.pdf)

# Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 13 January 2025*

Yes.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (Article 4(12) GDPR).

# Controllers/Owners have to notify:

*Last review date: 13 January 2025*

☒  data protection authorities

in case of a personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons

without undue delay and, where feasible, not later than 72 hours after having become aware of it (Article 33, GDPR).

☒  cybersecurity authorities

Under the NIS Regulations Operators of Essential Services and Digital Service Providers must notify CSIRT of any event having an actual adverse effect on the security of network and information systems that has a significant impact on the continuity of an essential service. Such an event *could* include a serious personal data security breach. (See further detail on obligations under the NIS Regulations on notification below).

☒  affected individuals

without undue delay

if a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, unless any of the following conditions are met:

the controller has implemented technical and organizational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption, or

the controller has taken subsequent measures that ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialize, or

it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34, GDPR).

# Processors/Agents have to notify:

*Last review date: 13 January 2025*

☒   controller/ owner

in case of a personal data breach irrespective of a risk to the rights and freedoms of the data subjects

without undue delay after becoming aware of it

# Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 13 January 2025*

Yes.

☒        cybersecurity authorities
☒         financial services requirements
☒        telecommunication requirements
☒        providers of critical infrastructure

**Details regarding the identified data security breach notification requirements**

Telecommunication requirements

The breach notification requirements of the ePrivacy Regulations 2011 (S.I. 336/2011) and EU Commission Regulation (No. 611/2013) apply to providers of publicly available electronic communications networks or services (i.e., Telecoms and ISP providers). A "personal data breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the European Union."

Where there has been a personal data breach, the provider has a mandatory obligation to notify (a) the DPC of the breach, and (b) an individual, where the breach is likely to adversely affect his or her personal data or privacy. An individual does not need to be notified if the provider has demonstrated to the DPC that it has implemented appropriate technological measures which render the data unintelligible to any person who is not authorized to access it.

An initial notification of a personal data breach must be made to the DPC no later than 24 hours after detection of the breach. If the provider is unable to provide full details on the breach at this time, further details should be provided within three days of the initial notification. If after this three day period, a provider is still unable to provide the full information required by the EU Regulation on the data security breach, it will be required to submit a reasoned justification as to why the information is not available. The information which must be provided in the notification is set out in Annex I of the EU Regulation.

Any notification to an individual adversely affected by the breach should be made "without undue delay" after detection of the personal data breach. The notification to the individual should include the information set out in Annex II of the EU Regulation.

Failure to notify is a criminal offence, punishable on summary conviction to a Class A fine (i.e., EUR 5,000), or on indictment to a fine up to EUR 250,000 in the case of a corporate body, or up to EUR 50,000 in the case of a natural person.

**Providers of critical infrastructure, financial services requirements and cybersecurity authorities**

As noted above, the NIS Regulations transposed the NIS1 Directive into Irish law. The Regulations apply to Operators of Essential Services (OESs) (i.e. critical infrastructure operators, which includes certain financial service providers) and Digital Service Providers (DSPs). They impose two primary obligations on OESs and DSPs: (a) to comply with relevant security requirements and (b) to notify relevant incidents to CSIRT.

A reportable incident is any incident which has a significant impact on the continuity of an essential service which an OES provides, or on the provision of a digital service that a DSP provides, within the EU. The incident notification must be made within 72 hours of the OES or DSP becoming aware of the incident. After consulting the relevant OES or DSP in relation to an incident, the CSIRT may inform the public about the incident or may require a DSP, where applicable, to inform the public of the incident.

Failure to notify the CSIRT of a reportable incident is an offence, punishable on summary conviction to a Class A fine (EUR 5,000) or on conviction on indictment to a fine not exceeding EUR 50,000 in the case of an individual, and EUR 500,000 in the case of a body corporate.

The requirements of the NIS2 Directive have not yet been transposed into Irish law however we expect this transposition will be completed in 2025. An overview of the NIS2 Directive is provided in the EU Chapter.

The EU’s Digital Operational Resilience Act Regulation (EU) 2022/2554 (**DORA**), as well as Directive (EU) 2015/2366 on payment services in the internal market, the revised Payment Services Directive (“**PSD2**”), impose specific cyber resilience and reporting obligations on in-scope organizations in the financial services sector.

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.