Global Data and Cyber Handbook - EU

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: 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
☒   requirement to undertake third party due diligence (security assessment of third party providers)

Art. 5(1)(f) and 32 GDPR impose a general obligation to take appropriate / reasonable technical, physical and/or organizational security measures.

Encryption is not a strict legal requirement, but encryption is considered by the GDPR as an appropriate technical and organizational measure.

Although undertaking processor due diligence is not a GDPR requirement as such, under Art. 28 GDPR, data controllers must only use processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the GDPR requirements.

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

*Last review date: January 2025*

**Yes**

☒   network information security requirements (broader than telecommunications)

☒   financial services requirements

☒   providers of critical infrastructure

☒   digital or connected (IOT) products

The NIS2 Directive, via national implementing law, imposes obligations on providers or critical infrastructure to protect systems from cyberattack. The scope of NIS2 is broad and may encompass public listed companies, and companies in the health, financial services or telecommunications sectors.

DORA, as well as the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, the revised Payment Services Directive (“**PSD2**”), impose specific cyber resilience and reporting obligations on in-scope organisations in the financial services sector.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (“**European Electronic Communications Code**”) imposes detailed security requirements for electronic communication providers.

The **Cyber Resilience Act** of 25 September 2024 will introduce new obligations on manufacturers, importers and distributors of products with digital elements designed to ensure the cybersecurity of such products. The Cyber Resilience Act will take effect in stages, with the obligation to notify actively exploited vulnerabilities for in-scope products taking effect from 11 September 2026 and the remaining obligations from 11 December 2027.

# 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?

N/A

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

*Last review date: January 2025*

Yes

# Controllers/Owners have to notify:

*Last updated date: January 2025*

☒   data protection authorities

☒   affected individuals

"Personal data breach" is defined under the GDPR 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.

Under the GDPR, the controller must notify the **competent supervisory authority** of a personaldata breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The controller must notify the **data subject** of a personaldata breach if it is likely to result in a high risk to the rights and freedoms of natural persons, without undue delay, unless:

the controller has implemented appropriate technical and organisational protection measures to the personal data affected, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

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.

# Processors/Agents have to notify:

*Last review date: January 2025*

controller/ owner

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

*Last review date: January 2025*

Yes

☒   cybersecurity authorities

☒   financial services requirementst

☒   providers of critical infrastructure

The NIS2 Directive, via national implementing law, imposes obligations on providers or critical infrastructure to protect systems from cyberattack and notification obligations. The scope of NIS2 is broad and may encompass public listed companies, and companies in the health, financial services or telecommunications sectors.

DORA, as well as the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 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.

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (“**European Electronic Communications Code**”) imposes detailed security requirements and notification obligations for electronic communication providers.

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.