NAVIGATING CYBERSECURITY REPORTING OBLIGATIONS IN THE EU AND THE UK

APRIL 2024

Weil

The cybersecurity legal landscape is getting busier. In response to the increase in cyber-attacks and threats on organisations in the EU and UK, a wealth of new (or updated) cybersecurity-related laws have been introduced or are on the horizon, including the EU Network and Information Security 2 Directive ("**NIS 2 Directive**") and the EU Digital Operational Resilience Act ("**DORA**"), the impact of each which will also be felt beyond the EU.

In particular, organisations in scope will need to consider any new incident report obligations alongside existing incident reporting obligations (such as under the GDPR/ UK GDPR) and how to operationalise these different notification obligations into security response plan and protocols, especially for broader notification triggers and shorter timelines.

Below is a table setting out a high-level summary of some of the key cybersecurity-related laws in the EU and the UK that contain incident reporting obligations, and how they compare to each other and the GDPR/ UK GDPR, along with some key takeaways for organisations to keep in mind.

KEY TAKEAWAYS

1. **Determine whether your organisation is in scope.** Determine whether your organisation is in scope of the relevant legislation. UK and other international entities may be in scope of the NIS 2 Directive and DORA. Equally, EU and other international entities may be in scope of UK NIS Regulations (including any updated regulation – see Key Takeaway 3 below).
2. **If DORA applies, certain obligations under the NIS 2 Directive may not.** If your organisation is in scope of both the NIS 2 Directive and DORA, you may only need to comply with the reporting obligations under DORA. This is because the NIS 2 Directive provides that certain obligations under the NIS 2 Directive will not apply where sector-specific laws lay down obligations which are at least equivalent (and specifically confirms that DORA is an example of such sector-specific legislation). However, note that the NIS 2 Directive becomes effective before DORA.
3. **Monitor for updates to the UK NIS Regulations.** The UK Government has announced it intends to update and expand the scope of the current UK NIS Regulations. This will include managed IT service providers and impose more stringent incident reporting obligations, similar to the NIS 2 Directive. If this is relevant to your organisation, monitor closely for updates.
4. **Don't forget about personal data.** If personal data is involved and you are in scope of the GDPR/ UK GDPR, then GDPR/ UK GDPR notifications obligations will apply to reportable breaches. You will also need to assess the incident from a personal data-centric perspective.
5. **Update incident response plans and protocols.** These may need to factor in shorter timeframes for notification under the NIS 2 Directive (in comparison to the existing EU NIS Directive) and reporting to third parties. More generally, ensure that your incident response plans are well-structured and straightforward, clearly specify roles and responsibilities, and are clear as to the information that should be shared with internally and externally. A robust incident response plan may also be something cyber insurance carriers require.
6. **Consider cyber insurance:** Incident response plans should also clearly state how and when to engage cyber insurance coverage. Response protocols may also be dictated by the cyber insurance in place.
7. **Conduct table top exercises.** Conduct table top exercises with scenarios that would require notifications under these new requirements to be better prepared for the short timeframe within which key decisions must be made. This can be crucial for identifying gaps in any incident response plans and rectifying them.
8. **Regulators talk - be consistent.** Regulators will be talking to each other. Be consistent in the content of your notifications when reporting the same incident to different regulators.
9. **Stakes are high (because fines are high).** While fines are not all at GDPR/ UK GDPR levels, the stakes are still as maximum fines are not insignificant.
10. **Other reporting obligations may also apply.** The below table is not exhaustive. Organisations may be subject to other sector-specific incident reporting obligations, e.g. payment service provider reporting obligations to the UK Financial Conduct Authority or under other cybersecurity–related legislation such as the EU Cyber Resilience Act (or even further afield than the UK or EU, such as reporting obligations to the SEC).

	EU Network and Information Security 2 Directive ("NIS 2 Directive")	**UK Network and Information Systems Regulations 2018 ("UK NIS Regulations")**	**EU Digital Operational Resilience Act ("DORA")**	**EU and UK General Data Protection Regulation ("GDPR/ UK GDPR")**
Focus	▪ Security of systems	▪ Security of systems	▪ Operational resilience	▪ Personal data
Timing	▪ Applies from 18 October 2024 (where implemented by EU Member States, which have 17 October 2024 implementation deadline). ▪ Replaces the first EU NIS Directive, significantly expanding its scope.	▪ In force since 10 May 2018. ▪ The UK NIS Regulations are based on the first EU NIS Directive. The UK Government has announced it intends to update the UK NIS Regulations.	▪ Applies from 17 January 2025.	▪ In force since 25 May 2018.
Who does it apply to?	**Sector Specific:** Essential and important entities that provide critical or important services in certain key sectors, including (for essential entities) energy, transport, banking, financial market infrastructure and digital infrastructure and ICT service management. (for important entities) manufacturing, and post and courier). Applies to all non-EU entities offering or operating such services in the EU.	**Sector Specific:** Entities that provide critical services in 5 key sectors (including energy, transport, health, and digital infrastructure) and digital service providers. *It is expected this will be expanded to include managed IT service providers.* Applies to non-UK digital service providers that offer services in the UK.	**Sector Specific:** Financial Sector. Covers almost the entire financial sector. Applies to non-EU entities if operating in the EU financial activities falling under its scope.	Not sector specific. Applies to all organisations in scope (those processing personal data in the EU or UK or caught by the extra-territorial provisions, e.g. if processing personal data as part of offering goods and services to, or monitoring behaviour of, individuals in the EU/UK.)
	Examples: (essential) data centre service providers, internet/mobile network providers, banks; pharmaceutical companies, managed IT service providers, (important): social media platforms postal and courier service providers, manufacturers of certain critical products, e.g. medical devices, computer, electronic and optical products, motor vehicles.	*Examples: healthcare providers, providers of cloud computing services and online marketplace and search engine services.*	*Examples: banks, payment service providers, investment fund managers, insurance companies, crypto exchanges, crowdfunding service providers, AIF managers, occupational pension schemes.*	

	EU Network and Information Security 2 Directive ("**NIS 2 Directive**")	UK Network and Information Systems Regulations 2018 ("**UK NIS Regulations**")	EU Digital Operational Resilience Act ("**DORA**")	EU and UK General Data Protection Regulation ("**GDPR/ UK GDPR**")
Relevant incidents	**Significant incidents**, meaning, broadly, incidents affecting systems which has caused or is capable of causing severe operational disruption of the services or financial loss, or considerable material or non-material damage to other persons. **Significant cyber threats**, meaning broadly, a cyber threat which based on technical characteristics can be assumed to have the potential to have a severe impact on systems of the entity or users of the service by causing considerable material or non-material damage.	**Incidents having a significant or substantial impact**, meaning, broadly, any event which has an actual adverse effect on the systems affecting the provision of the essential service or digital services. *However, the UK Government has announced that it intends to broaden the scope of reportable incidents, to include incidents that could impact services.*	**Major ICT-related incidents**, meaning, broadly, incidents that have a high adverse impact on systems that support critical or important functions. **Significant cyber threats**, meaning broadly, a cyber threat which based on technical characteristics can be assumed to have the potential to have a severe impact on systems of the entity or users of the service by causing considerable material or non-material damage. *Regulatory technical standards have been published by the European Supervisory Authorities to assist with classifying any incidents.*	Personal data breaches. *However, note that not all personal data breaches are notifiable to a regulator or data subjects: it depends upon risk (see further below).*
Reporting obligations to regulators	**Significant incidents:** Report significant incidents to the Member State Computer Security Incident Response Team (CSIRT) or the competent authority in multiple stages: 1. Early Warning Notification – 24 hours: 2. Incident Notification – 72 hours: 3. Final Report – 1 month of submitting the incident notification (or if the investigation is ongoing then a progress report must be submitted within 1 month of the incident notification and a final report submitted within 1 month of the handling of the incident).	**Incidents having a significant or substantial impact** must be notified to the relevant regulator within 72 hours of becoming aware.	**Major ICT-related incidents:** Report to the relevant competent authority (will depend upon the financial entity). 1. Initial Notification, as early as possible within 4 hours from the moment of classification of the incident as major, but no later than 24 hours from the time of detection of the incident. 2. Intermediate Report – within 72 hours from the classification of the incident as major, or when regular activities have been recovered and business is back to normal. *(Continues)*	Notify the relevant data protection regulator within 72 hours of becoming aware, *unless* that personal data breach is unlikely to result in a risk to the rights and freedoms of the affected data subjects.

	EU Network and Information Security 2 Directive ("**NIS 2 Directive**")	UK Network and Information Systems Regulations 2018 ("**UK NIS Regulations**")	EU Digital Operational Resilience Act ("**DORA**")	EU and UK General Data Protection Regulation ("**GDPR/ UK GDPR**")
			3. **Final Report** – no later than 1 month from the classification of the incident as major, unless the incident has not been resolved, in which case it will be the day after the incident has been re-solved permanently. *Timeframes reflect those set out in the draft regulatory technical standards. These may be subject to change*	
Reporting obligations to third parties	▪ **Significant incidents:** Notify service recipients without undue delay where the provision of services is likely to be adversely impacted. Also inform of any ▪ **Significant cyber threats:** Inform service recipients that are potentially affected without undue delay of any measures they can take to mitigate the resulting risk and, where appropriate, of the actual cyber threat itself, e.g. where the cyber threat is likely to materialise.	None.	▪ **Major ICT-related incidents:** Inform **clients** without undue delay of the incident and (where the incident has an impact on the financial interests of the client). ▪ **Significant cyber threats:** Inform clients that are potentially affected of any appropriate protection measures that they may consider taking.	Data controllers must notify affected data subjects without undue delay upon becoming aware, *but only if* the breach is likely to result in a high risk to their rights and freedoms.
Sanctions	▪ Failing to comply with the reporting obligations, maximum fine of (i) for essential entities, €10 million or up to 2% of annual global turnover; (ii) for important entities €7 million or up to 1.4% of annual global turnover whichever is greater.	▪ Failing to report an incident could attract a maximum fine of £17 million.	▪ Maximum fines to be determined by Member States.	▪ For failing to report a breach, maximum fine of €20 million (£17.5 million) or 4% of the annual global turnover, whichever is greater.

FOR MORE INFORMATION

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

BARRY FISHLEY

+44 20 7903 1410
barry.fishley@weil.com

CHLOE KITE

+44 20 7903 1206
chloe.kite@weil.com

WEIL.COM

#97864250

Weil