RPC

Navigating a cyber breach

Fulfilling a company's notification obligations in the event of a cyber incident is becoming an increasing challenge. Businesses must satisfy a range of statutory, regulatory and contractual notification requirements, often with differing thresholds, timescales and formats. This article summarises some of the notification obligations that can arise in the context of a cyber incident, as well as some of the key changes coming down the track.

Upcoming legislation

There has been much talk of the new bills recently proposed by the UK's Labour government:

- The Cyber Security and Resilience Bill – intended to strengthen the UK's cyber defences, mandate increased cyber incident reporting, and give greater powers to regulators.
- The Data (Use and Access) Bill – which amends certain provisions of the UK GDPR, the Data Protection Act 2018, and others.
- The AI Bill – said to enhance the legal safeguards surrounding the most cutting-edge AI technologies.

Businesses will need to consider their obligations once the new bills come into force. In particular, it is said that the Cyber Security and Resilience Bill will increase mandatory incident reporting in the event of a cyber incident for a broader range of organisations than is currently the case.

We wait in eager anticipation for further guidance from the government. In the meantime, this article can be used as a roadmap for some of the key notification obligations that could arise in the context of a cyber incident.

Authors

Rachel Ford
Partner
+44 20 3060 6821
rachel.ford@rpc.co.uk

Emanuele Santella
Associate
+44 20 3060 6023
emanuele.santella@rpc.co.uk

Key notification obligations in the context of a cyber incident

UK General Data Protection Regulation (UK GDPR)

Who is caught?

Any organisation that suffers a personal data breach. A personal data breach involves a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (any information relating to an identifiable individual) (Art 4(1) and (12), UK GDPR)

Notification obligations:

- If you are a Data Controller:
  - A notification must be issued to the ICO within 72 hours of becoming aware of a personal data breach, unless it is unlikely to result in a risk to the rights and freedoms of individuals (Art 33(1), UK GDPR).
  - Notifications must be issued to individuals without undue delay if a personal data breach is likely to result in a high risk to their rights and freedoms (Art 34(1) UK GDPR).
- If you are a Data Processor:
  - A notification must be issued to a Data Controller without undue delay after becoming aware of any personal data breach, regardless of the level of risk to individuals (Art 33(2) UK GDPR).

Network and Information Systems Regulations (NIS)

Who is caught?

All businesses that are subject to the NIS Regulations: Operators of Essential Services ("OES")[1] and Relevant Digital Service Providers (RDSPs)[2]. The notification obligations under NIS are relevant to any breach of security, regardless of whether personal data is concerned. Businesses will be exempt from NIS if they have less than 50 staff and an annual turnover or a balance sheet of less than €10m.

Notification obligations:

- For an OES, notification must be made to the OES' regulator within 72 hours of them becoming aware of an incident which has a significant impact on the continuity of their essential service (Reg 11(1)-(3), NIS).
- For an RDSP, notification must be made to the ICO within 72 hours of them becoming aware of an incident which has a substantial impact on the provision of their digital services (12(3) and 12(6), NIS).

Payment Card Industry Data Security Standard (PCI DSS)

Who is caught?

Any business which holds and processes payment card data relating to Amex, Discover, JCB, Mastercard and VISA cards.[3]

Notification obligations:

- Notification obligations vary across each card issuer. By way of example, Amex requires notification within 72 hours of discovery of a Data Incident (a potential or confirmed compromise of information belonging to American Express Card Members). The key point is that there are often tight timescales (24 hours in some cases), standardised forms and specific contact addresses.

1. Operators of Essential Services are organisations that operate services deemed critical to the economy and wider society. They include critical infrastructure (water, transport, energy) and other important services, such as healthcare and digital infrastructure (Reg. 1(2)).
2. Relevant Digital Service Providers are organisations that provide specific types of digital services: online search engines, online marketplaces and cloud computing services (Reg. 1(2)). To be an RDSP, you must provide one or more of these services, have your head office in the UK (or have nominated a UK representative) and be a medium-sized enterprise.
3. Can be viewed here

Welcome
UK GDPR
NIS regulations
PCI DSS
PECR
TSA
PSTI
EIDAs
Specific contractual obligations
Broader regulator obligations
Law enforcement
Contacts

Key notification obligations in the context of a cyber incident

Privacy and Electronic Communications Regulations (PECR)

Who is caught?

For the purposes of the notification obligations, providers of public electronic communications services or networks ('service providers').

Notification obligations:

- A service provider must notify the ICO within 24 hours and without undue delay after becoming aware of a personal data breach (Reg 5A(2), PECR).
- Notification might also need to be made to users[4] and/or subscribers[5], if the personal data breach is likely to adversely affect their personal data or privacy (Reg 5A(3)-(6), PECR).

Telecommunications Security Act 2021 (TSA)

Who is caught?

For the purposes of the notification obligations, providers of public electronic communications networks and services ('service providers'").

Notification obligations:

- Service providers must notify OFCOM as soon as reasonably practicable of certain, defined security compromises. This includes (a) any security compromise that has a significant effect on the operation of the network or service, and (b) certain, defined security compromises that put any person in a position to be able to bring about a further security compromise that would have a significant effect on the network or service[6].
- Service providers must notify users (a) where there is a significant risk of a security compromise occurring in relation to the network or service, and (b) where users may be adversely affected by the security compromise[7].

Product Security and Telecommunications Infrastructure Act 2022 (PSTI)

Who is caught?

Manufacturers[8], importers[9], and distributors[10] of internet and network-connectable consumer products.

Notification obligations:

- Specific notification obligations for each of the entities caught by the Act are triggered in the event of a compliance failure relating to product security, ie a failure to comply with the specific compliance and security requirements set out in the Act.
- The notification obligations are complex. There are obligations to notify the relevant enforcement authority (the OPSS in the UK), respective manufacturers/importers/distributors as well as impacted customers depending on the circumstances of the compliance failure.
- In our experience, a cyber incident can highlight the fact that a compliance failure has occurred, which in turn prompts the notification obligations.

4. A user is any individual using a public electronic communications service (Reg 2(1)).
5. A subscriber is a person who is a party to a contract with a provider of public electronic communications services for the supply of such services (Reg 2(1)).
6. s.4(2) ("105K Duty to inform OFCOM of a security compromise")
7. s.4(2)("105J Duty to inform users of risk of security compromise")
8. A manufacturer is a person who manufactures a product or has a product designed or manufactured and markets that product under a proprietary name or trademark AND/OR any person who markets a product manufactured by another person under its own name or trademark (s7(3)).
9. An importer is any person that imports products into the UK and is not a manufacturer of the products (s7(4)).
10. A distributor is any person that makes the product available in the UK and is neither a manufacturer nor importer (s7(5)).

Welcome
UK GDPR
NIS regulations
PCI DSS
PECR
TSA
PSTI
EIDAs
Specific contractual obligations
Broader regulator obligations
Law enforcement
Contacts

Key notification obligations in the context of a cyber incident

Electronic Identification and Trust Services for Electronic Transactions Regulations (EIDAs)

Who is caught?

Any natural or legal person offering trust services via electronic seals, electronic signatures, electronic time stamps, electronic registered delivery services and certificate services for website authentication.

Notification obligations:

- Notification must be made to the ICO within 24 hours of a business becoming aware of any breach of security or loss of integrity to the trust service, if that has a significant impact on the service or on the personal data maintained therein (Article 19(2)). Notification is expected sooner than 24 hours if it is reasonable to do so.
- Where the breach of security or loss of integrity to the trust service is likely to adversely affect a natural or legal person to whom the trust service has been provided, the trust service provider must also notify the natural or legal person of the incident without undue delay (Article 19 (2)).

Specific contractual obligations

Who is caught?

Any business that contracts with third parties (customers, clients, suppliers etc) should consider the terms of the contracts, in particular, whether the contracts contain notification obligations in the event of a cyber incident.

Notification obligations: Vary across each contract but our experience is that these notification obligations can be reasonably broad (the trigger can be 'in the event of a suspected security incident') and there are often tight timescales (24 hours in some cases) with specific notice requirements.

Broader regulatory obligations

Any business that suffers a cyber incident should also consider their notification obligations to any regulators specific to their sector. This includes, for example, the SRA, FCA and Charity Commission. In our experience, these regulators might need to be notified in the event of a cyber incident, particularly in circumstances whereby the ICO is being notified.

Law enforcement

Who is caught?

All businesses.

Notification obligations: Subject to the specific circumstances and depending on its complexity, law enforcement encourage notification of a cyber incident and there are benefits to doing so. Whilst it will depend on the specific circumstances, there are reporting channels to Action Fraud, the National Cyber Security Centre and the National Crime Agency.

Contacts

Richard Breavington
Partner
+44 20 3060 6341
richard.breavington@rpc.co.uk

Daniel Guilfoyle
Partner
+44 20 3060 6912
daniel.guilfoyle@rpc.co.uk

Rachel Ford
Partner
+44 20 3060 6821
rachel.ford@rpc.co.uk

For further guidance, both in respect of managing a breach and preparing as best you can in advance of that risk, please feel free to reach out to RPC's cyber team. Full details of our expertise can also be found on our website and via our very own app RPC Cyber available for free from the Apple Store and Google Play.

Disclaimer

The information in this publication is for guidance purposes only and does not constitute legal advice. We attempt to ensure that the content is current as of the date of publication but we do not guarantee that it remains up to date. You should seek legal or other professional advice before acting or relying on any of the content.

rpclegal.com