THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

# Legal Implications of a Cyber Incident

In partnership with

Scottish Business Resilience Centre

NORTH WEST REGIONAL ORGANISED CRIME UNIT

irwinmitchell

nwcrc.co.uk

# Legal Implications of a Cyber Incident

Just as every cyber incident is unique, so too is the way a cyber incident must be managed in order to mitigate the risks it poses to your business.

**However, you do not need to reinvent the wheel each time. Awareness of the key commercial and legal implications of a cyber incident is key to responding appropriately to any incident and mitigating the risks arising from it. Here are some points to consider, to help ensure the decisions you take during and in the aftermath of a cyber incident enable you to navigate out of choppy waters with minimal damage.**

## Insurance / Crisis Response Plan

Do you have a plan for dealing with the incident?

Having a plan in place before an incident occurs removes a lot of the stress from managing the response. If you have cyber insurance, you should notify your insurer of an incident as soon as possible. Not only will this avoid the difficulties of retrospective insurance claims, but many cyber policies offer customers access to a team of incident response specialists (IT technical consultants, legal consultants, PR consultants etc) who will be able to support insured organisations through the key investigations, decisions and responses that will need to be made. Whether you have cyber insurance, having a Cyber Incident Response Plan – and knowing where to access it – will also provide you with a road map to help with decision-making.

## Regulatory notification obligations

Consider what regulators your business owes obligations to, and particularly reporting requirements – what you have to report, to whom and when.

Owing to the nature of the information regulators require to be advised of, prioritising regulatory investigations will not only help mitigate the risk of regulatory penalties and fines, but will also help you clarify information that is likely to be critical to other urgent communications (e.g. communications to data subjects, to staff, to third party contractors, to the public etc).

The main regulatory obligations to be aware of in the event of a cyber incident are those triggered by a personal data breach in terms of the UK General Data Protection Regulations (UK GDPR). The UK GDPR applies to all organisations providing goods and services in the UK.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It can broadly be described as a security incident that has affected the confidentiality, integrity or availability of personal data. Not all security incidents are personal data breaches.





If a personal data breach has occurred, you will probably need to notify the Information Commissioner's Office (ICO), and you may need to notify affected data subjects.

## Notifying the Information Commissioner's Office

### Who is responsible for notifying?

**The obligation to notify is on the data controller. The data controller determines the purposes and means by which data is processed.**

- Contrast this with a data processor, which processes data in accordance with instructions of the date controller. A data processer is obliged to notify the data controller of any personal data breach "without undue delay" (but beware stricter contractual obligations – more below).

### When?

**Without undue delay, and in any case within 72 hours after having become aware of the personal data breach.**

- A data controller is deemed to have "become aware" when it has a "reasonable degree of certainty" that the incident affects personal data.
- If you do not have all the information, the notification can be made in stages (without undue further delay).

### In what circumstances?

**Notification is required unless the personal data breach is "unlikely to result in a risk to the rights and freedoms of natural persons".**

- Consider the type of breach; the nature, sensitivity and volume of personal data; consequences for individuals; special characteristics of individuals; and characteristics of the data controller.
- Presumption of "high risk" if the personal data breach involves special categories of data, e.g. race and ethnic origin; religious or philosophical beliefs; political opinions; trade union memberships; biometric data used to identify an individual; genetic data; health data; and data related to sexual preferences, sex life, and / or sexual orientation.
- Examples of risks to rights and freedoms include; loss of control of personal data; identity theft or fraud; financial loss; unauthorised reversal of pseudonymisation; damage to reputation; loss of confidential information protected by professional secrecy; and other significant economic or social disadvantage to the natural personal concerned.

### Who?

**Notification should be made to the Information Commissioner's Office (ICO).**

- If the organisation carries out cross-border processing with any EU member states, the European GDPR may apply in which case a separate notification may be required to the relevant EU member state's supervisory authority, again within 72 hours.
- Where multiple member states are involved, the 'One-Stop-Shop' system within the EU may allow a single supervisory authority within the EU to act as the lead on behalf of other EU supervisory authorities.
- If the organisation carries out cross-border processing in other parts of the world, it should take local law advice on reporting requirements.

### How?

**A notification can be made by telephone, or in writing via the personal data breach reporting form available on the ICO website.**

- If notifying by the telephone, prepare a script in advance. Focus on remedial steps taken to protect data subjects and the timeline for when the steps will be implemented.

## Notifying affected Data Subjects

### In what circumstances?

**Notification is required if the personal data breach is "likely to result in a high risk to the rights and freedoms of natural persons".**

- This is a higher threshold than for ICO notification as it is designed to protect individuals from unnecessary notification fatigue.
- Assess the severity and potential or actual impact on individuals.

### How?

**A dedicated notification in clear and plain language.**

- Ensure that the message is accurate and consistent.
- Press releases or general media statements are unlikely to be viewed as effective unless there is no other means of contacting the individual. However, if individual notification would involve a disproportionate effort, a public communication may suffice if "equally effective".

### When?

**Without undue delay after having become aware of the personal data breach.**

- Consider whether to prioritise vulnerable customers.
- Ensure that an appropriate framework is in place to respond to customer queries or complaints i.e. a call centre, FAQ answers for call handlers etc.

### What?

**The notification should include:**

1 The name and contact details of your Data Protection Officer or other contact.

2 A description of the likely consequences of the personal data breach.

3 A description of the measures taken, or proposed to be taken, in response.

- Advise data subjects on any steps they can take to mitigate risk.
- Consider whether to offer customer redress, including services such as ID theft protection and credit monitoring.

- Other sector-specific notification requirements exist for certain businesses, particularly those in the financial services, telecoms and health sectors. Ensure you are aware of whether any of those apply to your business.

### Contractual obligations

A cyber incident is likely to trigger certain contractual obligations, and may impede the performance of others.

For example, an incident is likely to trigger a data processor's contractual obligation to notify the data controller, and it may also prevent a business from fulfilling customer orders if critical business systems are unavailable. Failure to respond promptly and positively in either situation could increase the risk of your business facing claims for breach of contract. To mitigate that risk, the main types of contract to consider are:

Controller / processor contracts: although the UK GDPR requires data processors to notify controllers of a personal data breach "without undue delay", controller / processor contracts often shorten this to 24 hours.

So check any controller / processor contracts, especially if you are the processor.

Third-party supplier contracts: has the incident affected your organisation's ability to meet any contractual obligations? You may have contractual obligations to notify others in your supply chain if a cyber incident occurs or your ability to perform particular obligations is compromised.

Customer contracts: if critical systems are affected, cyber incidents can interrupt the usual processing and fulfilment of customer orders. If significant delays or cancellations are likely, consider how you will prioritise order fulfilment to mitigate customer claims, and how you will communicate with customers to maintain customer confidence.





### Litigation risk

Since 2018, the litigation risk arising from a cyber incident has significantly increased for businesses.

The UK GDPR came into force, giving consumers affected by a data breach / cyber incident more legal remedies against organisations holding their data; and Scotland introduced its first "class actions" procedure, making mass claims a real possibility in the event of mass-harm events such as data breaches or cyber incidents.

Since 2018, we have seen a marked increase in the number of legal claims being made against businesses that have, directly or indirectly, suffered a cyber incident. Whether well-founded or spurious, the significant "costs" of litigation – including management time, adverse publicity, stress, and of course legal costs – can be felt by an organisation long before a court is asked to decide if damages should be ordered.

The best way to minimise litigation risk is by (a) implementing and maintaining appropriate technical and organisational measures to ensure adequate security, and (b) understanding and preparing to respond promptly and positively to the legal and contractual implications of a cyber incident. Sometimes, however, claims will arise despite your best efforts. By taking strategic legal advice at an early stage, many such claims can be seen off, or resolved at a low value. For more persistent claims, or where there is a risk of class action, early litigation advice will be essential to mitigating your exposure.

### What next?

Cyber incidents need to be regarded as a "when", not an "if".

As planning and preparation is key to managing the incident in a way that helps you mitigate the risks posed by your regulatory, contractual and legal obligations, prepare your incident response plan in advance so you have a route map to follow when the time comes. Keep the plan under review. If an incident occurs, review your response plan in light of it and update the plan where necessary. If any claims are made against your organisation, seek strategic legal advice at an early stage, to help identify those claims which can be relatively swiftly headed off or resolved, and to devise early anti-proliferation and defence strategies for those which are more complicated.

This document was produced with support by Irwin Mitchell. For legal advice in relation to a cyber incident, or for more information on managing litigation risk in relation to an incident, please contact Irwin Mitchell at **www.irwinmitchell.com/contact-us** or via phone on **0808 302 3839**.

Designed by

Agent.

THE CYBER RESILIENCE CENTRE FOR THE NORTH WEST

Cyber Resilience Centre
Manchester Technology Centre
Oxford Rd
Manchester
M1 7ED

0161 706 0940

info@nwcrc.co.uk

nwcrc.co.uk

@northwestcrc