PERSONAL DATA BREACHES

All breaches great and small

Assessing the risk from a data breach

Publication date: March 2022

Sponsored by exterro®

DPN DATA PROTECTION NETWORK

© 2022 Copyright of Data Protection Network. All rights reserved.

Contents

Back to contents

Copyright of Data Protection Network. All rights reserved. 2022 ©

Foreword

The stakes are high. With the clock ticking to meet the 72-hour breach reporting timeline, it's vital your plans are in place and the response is rapid and effective.

Under UK/EU GDPR a personal data breach must be reported to a Supervisory Authority within 72-hours of becoming 'aware' of it, unless it's unlikely to represent a 'risk' to individuals. Affected individuals must be informed where there's a 'high risk'.

Pre-GDPR, the UK's Information Commissioner's Office (ICO) received around 750 breach reports each quarter. Post May 2018, this peaked at more than 3,000 per quarter but has now settled at around 2,500. To date, of all reported events, 66% are non-cyber incidents (latest update mid 2021). This trend is reflected across Europe.

Commissioner John Edwards says the ICO saw a 'steady and significant' rise in cyber-attacks in the last six months of 2021.

Our *Privacy Pulse Report 2022* confirms data breaches are endemic, with 68% of those surveyed saying they'd suffered at least one data breach in the past year. In fact, 41% said they'd suffered eleven or more breaches in the year!

The ICO has indicated there's a degree of over-reporting. Is this driven by a fear of getting it wrong? Could reporting minor incidents reveal your organisation's lack of due process to triage and assess risks?

The UK Government's Autumn 2021 consultation paper on data reform proposed raising the threshold for breach reporting.

With so many breaches occurring, it can be a challenge to work out which incidents need to be reported and when to inform affected individuals. Sometimes this is a clear-cut decision, but often it's more nuanced.

That's exactly why we created this white paper - to help assess the risks posed by a data breach and to reach an objective decision on whether to report it or not.

DPN has discussed data breaches widely through our articles and webinars. You can find all our published content at *dpnetwork.org.uk*.

Robert Bond

Chair of Advisory Group
Data Protection Network

Copyright of Data Protection Network. All rights reserved. 2022 ©

1. Executive summary

Data breaches are endemic. This paper provides a step-by-step guide to assessing, tackling and reporting the risks posed.

It's designed to help you reach a decision on whether an incident meets the threshold to report to a Supervisory Authority and how to judge when affected individuals should be informed.

Getting organised in advance is essential – if a data breach occurs there's no time to start planning how to respond on the hoof.

Prepare

Develop a data breach procedure or playbook, test it and keep it under regular review

Training and awareness

Make sure everyone knows what a data incident looks like and what they need to do, even if they only suspect something might be wrong.

Incident response team

Assign a suitably knowledgeable data incident team and know who else might need to be pulled in to support. If you're a small business, have external experts on hand to support when required.

Methodology

Adopt a suitable way for assessing, evaluating and documenting risk.

Reporting

Know who to report to, what details they'd expect and key messages to convey to affected individuals. Reporting can be done in phases as information emerges.

Record keeping

Maintain a detailed log of all personal data breaches, whether they're judged to be reportable or not.

Justification

Keep a record of your reasons for not reporting.

Technology

Have cyber security plans in place including detection and prevention software.

This paper provides the detail necessary to start planning how you'll respond when the inevitable happens.

Back to contents ◁

Copyright of Data Protection Network. All rights reserved. 2022 ©

2. Core building blocks

2.1 Data incident or personal data breach?

A data incident may be defined as a security event which compromises the integrity, confidentiality, or availability of an information asset.

A data incident becomes a personal data breach when it involves personal data which can either directly or indirectly identify individuals. 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 transmitted, stored or otherwise processed.*” (GDPR, Article 4.12)

This may involve innocuous information; in other cases it will be more significant. The challenge is determining how risky the breach may be for those potentially affected and for your organisation, and deciding what action to take.

2.2 Common types of data breaches

2.2.1 Accidental disclosure

A mistake is made and personal data is shared with an individual or group who shouldn’t have access to it.

Often, this happens within the content of an email or an unprotected attachment, when someone accidentally types in the wrong recipient email address, or by openly cc’ing individuals rather than blind copying.

When this happens, you need to consider the volume and sensitivity of the data and your relationship with the other party or parties.

- Is it appropriate to contact the receiver(s) and ask them to delete the data immediately?
- If the receiver is not trustworthy, could contacting them potentially increase the risk, by alerting them to your mistake?

If the recipient is someone you know and trust, who can confirm they’ve deleted what they’ve received, the risk will generally be minimised.

ICO fine – HIV Scotland

An email was sent to members of HIV Scotland’s Community Action Network (CAN). Email addresses were accidentally made visible to all recipients in the ‘cc’ field. In this case 106 people were affected.

The ICO commented assumptions could be made about individuals’ HIV status or risk from the data disclosed. The ICO issued a fine of £10,000.

Copyright of Data Protection Network. All rights reserved. 2022 ©

2.2.2 Lost or stolen devices

Where a device (phone, laptop or tablet) has been lost or stolen, think about the following questions:

- What data did the individual have access to?
- What's the volume and sensitivity of affected data?
- Is data encrypted, or at least protected with a strong password or passcode?
- What other security measures are in place to protect the data (e.g. multi-factor authentication)?
- Is the data recoverable? If not, how significant is the loss?

2.2.3 Social engineering & identify theft

Social engineering is widespread. It's designed to fool people into revealing information or providing access to systems:

- **Phishing** is most common, where the attacker recreates a company's website or portal and then sends a link to people via emails or social media. The recipient may end up compromising their personal information, login credentials or perhaps even credit card or bank details.
- **Baiting** is where an attacker entices someone to take a certain action. For example, by posting download links online which contain malicious software, hoping someone will click on them.

These attacks can represent a high level of risk particularly if sensitive or financial data is compromised.

Personal data obtained could also be used to access an account within the organisation or used externally to exploit authentication measures in other organisations.

2.2.4 Ransomware

Where a bad actor uses a malicious code to encrypt an organisation's data. They may also exfiltrate (export) data from the host systems.

The usual pattern is for the attacker to ask the organisation for a ransom in exchange for the decryption code and an undertaking not to leak the data.

The difficulties this presents include:

- Can't access the data.
- Confirming whether data has been exfiltrated or not.
- What will happen if ransom isn't paid.

When assessing the risks from a ransomware attack, you need to try and identify the type of the malicious code used and its origin, to understand the possible consequences.

The risk to individuals (as well as damage to the organisation) is likely to result from the leaking of personal data by the bad actor. But you should also consider any inability to carry out routine operations if you can't access encrypted data.

Copyright of Data Protection Network. All rights reserved. 2022 ©

The organisation will need to reinstate the encrypted systems. Having full and regular backups in place will mitigate the effects of the breach.

Regardless of the outcome and consequences, re- evaluating IT security measures is critical for organisations who've suffered ransomware or other malicious attacks.

2.3 ICO breach reporting statistics

The ICO categorises the main types of reported breaches as cyber and non-cyber related. The most striking statistic is that, in the last quarter reported in 2021, 70% are non-cyber events.

Common non-cyber breaches – 70% total reported:

- ✓ Data emailed or posted to incorrect recipient – 24.2%
- ✓ Unauthorised non-cyber access – 8.6%
- ✓ Loss/theft of paperwork or data left in insecure location 6.7%
- ✓ Failure to redact personal information – 4.2%
- ✓ Failure to use bcc – 3.0%
- ✓ Verbal disclosure of personal data – 2.8%
- ✓ Loss/theft of device containing personal data 1.9%

Common cyber breaches – 30% total reported:

- ✓ Social engineering & phishing scams – 11.0%
- ✓ Ransomware with assumed exfiltration (export of data) – 9.0%
- ✓ Unauthorised access – 2.7%
- ✓ Hardware/software misconfiguration – 2.3%

2.4 Processor breaches

If a processor suffers a personal data breach, they must inform controller of the data affected 'without undue delay'.

This upwards reporting of a breach applies throughout the supply chain, from a sub-processor up to the processor above them (and so on) and up to the controller.

This enables organisations to take their own steps to address the breach and meet their Supervisory Authority reporting obligations.

Requirements to inform and provide assistance are normally detailed in contracts between controllers and processors, and between processors and sub-processors. If a data incident occurs, it's worth double checking your contractual obligations.

Processors need to provide as much information as possible, as quickly as possible as to the nature of what has gone wrong, who is affected, mitigating measures and so forth.

A processor may be held liable for non-compliance under the UK GDPR. It goes without saying being well prepared is as important for a processor as it is for a controller.

Back to contents ◁

Copyright of Data Protection Network. All rights reserved. 2022 ©

2.5 Data incident and breach planning

The level of sophistication of your incident handling procedures should be proportionate to the size of your organisation considering the sensitivity and volume of personal data handled.

A data incident playbook is a great way to provide all the necessary information to help walk through the stages of managing a data incident. Often, these steps may need to run concurrently.

Data incident playbook (example of contents)

Identification & internal reporting
Provide training and awareness so your people understand what to look out for, and make sure they know how to report data incidents.

Incident Response Team
Appoint Incident Response Team - key people who'll handle and lead the investigation. Make sure they're briefed. Build in flexibility to call on others for support when necessary.

Establish the facts
Adopt a process to gather key information about the nature and scale of the incident as quickly and efficiently as possible. Confirm if personal data is involved.

Triage and mitigation
If personal data is involved take steps to resolve or reduce the impact of the breach as quickly and as thoroughly as possible. Take care to not to delete evidence.

Assessment
Adopt a clear methodology for evaluating the scale and potential for harm to individuals. This would normally involve assessing both likelihood and severity of potential consequences.

Decision
A decision will need to be taken on whether to report the breach and/or inform affected individuals. This may may need to be done before all the facts are known. Know in advance who'll be responsible for making this decision.

Reporting
Breach reports and messaging to affected individuals must be transparent, informative and offer reassurance you're doing everything you can to rectify the issue and protect those affected. Being familiar with the ICO's breach reporting form and having templates to use/ adapt for affected individuals will save a last-minute panic.

Communications and reputation management
A joined-up, coherent pre-planned approach to internal and external communications can go a long way to minimising any reputational damage.

Post-incident review and learnings
Build-in a review process. Key learnings can be drawn from even the minor incidents. You may identify additional measures which can be taken to prevent future breaches occuring.

> “*The single most important thing an organisation can do in handling a breach is creating and maintaining a playbook. Second is practising it using tabletop exercises.*”
> **Ray Pathak, Vice President Data Privacy, Exterro**

Back to contents

Copyright of Data Protection Network. All rights reserved. 2022 ©

3. Assessing data breach risks

3.1 Making the decision to report or not

Deciding whether to report is a leadership challenge and will depend on your organisation's appetite for risk.

Sometimes it will be obvious you need to report and inform affected individuals. Other incidents clearly won't meet the reporting threshold. However, a breach may fall somewhere in the middle, requiring careful judgement.

What's clear is the ICO currently believes organisations are over-reporting although, the ICO is (rightly) leaving it to organisations to assess the risk and their own decision.

However, reporting every data breach, without considering its risk profile, is potentially as unhelpful as not reporting anything at all. The Supervisory Authority is left with the unenviable task of sifting through to find those which truly require attention.

> *"There's no exact science, or black and white rules for when or what to report. Each incident should be evaluated on the related facts. What you need to establish is a defensible position which your organisation is comfortable with."*
> **Ray Pathak, Vice President Data Privacy, Exterro**

Case study – Construction sector

An attempt was made to encrypt systems and exfiltrate data. A ransomware demand was received. It's not clear whether data has been stolen or what types of data.

Action: Measures taken to mitigate risk.

Assessment: Risk posed by malicious actors, although the true extent was not clear.

Decision: Reported to ICO within 72-hours, further details provided when available. Provided information for customers (due to exfiltration risk) and updated as necessary.

Case study – Hospitality sector

30 restaurant customers were emailed to let them know about roadworks affecting parking. The employee forgot to use bcc (blind-copy), so customers could see each other's email addresses.

Action: Sent an apology and request to delete.

Assessment: Minimal risk posed.

Decision: Breach report to ICO not required.

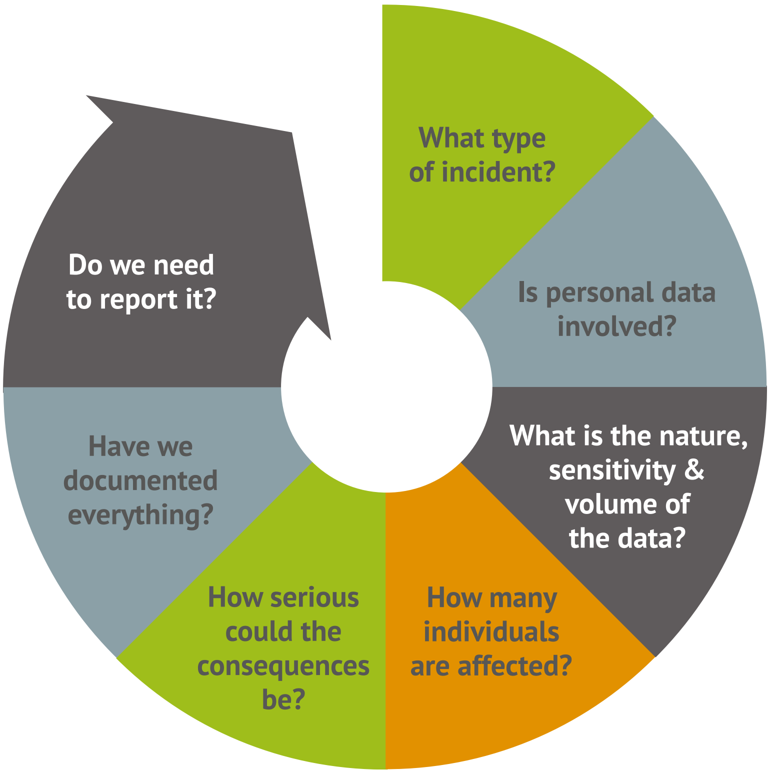
Copyright of Data Protection Network. All rights reserved. 2022 ©

Decisions about reporting revolve around two key questions:

- Does the breach really meet the threshold to report to the Supervisory Authority?
- Should we also inform affected individuals?

So how do you identify risks and assess them?

3.2 The seven-step assessment process


What type of incident?
Is personal data involved?
What is the nature, sensitivity & volume of the data?
How many individuals are affected?
How serious could the consequences be?
Have we documented everything?
Do we need to report it?

You need to make a rational and objective judgement based on the severity of the risks posed and the likelihood of these occurring.

Copyright of Data Protection Network. All rights reserved. 2022 ©

3.3 Establishing the precise circumstances of the breach

This sample, non-exhaustive, risk assessment questionnaire illustrates some of the factors to consider.

Question	Considerations	Comments (in separate boxes)
What type of incident is it?	**Accidental or malicious?** Is there a clear intention to cause harm? Has data been accessed or exfiltrated (stolen)?	▶ If a disgruntled ex-employee has stolen records, the intention to use this data maliciously could be obvious.
Is personal data involved?	**Are individuals directly or** indirectly identifiable? e.g. name, email address, customer id, payroll number. **How easy is it to identify people?** Would it take specialist knowledge or a decryption key?	▶ With ransomware attacks it's not always clear if personal data has been exfiltrated or not.
What is the nature, sensitivity and volume of the data?	**Who are the affected individuals?** Does who they are put them at greater risk? **How sensitive is the data?** Bank details, health records and biometric records will always represent a red flag. A combination of data may pose a greater risk than a single piece of information. **How many records?** Generally, the higher the volume, the greater the impact. But also consider how sensitive the data is.	▶ Names and postal addresses may seem unlikely to pose a risk, but it will depend on the context. ▶ A small volume of medical data may have more severe consequences than a large volume of non-sensitive data.
How serious could the consequences be for individuals affected?	Consider the nature of your business, the personal data involved and what you know about the intentions of who has the data.	▶ Consequences may be less severe where data is in the hands of a trusted party.

Back to contents ◁

Copyright of Data Protection Network. All rights reserved. 2022 ©

ICO fine – UK Government Cabinet Office

The inadvertent publication of postal addresses of recipients of the UK New Year's Honours List in 2019 represented a risk to personal safety because of the type of people concerned.

Clearly people in the public eye could have good reasons for not wanting their home addresses to be public knowledge.

This affected more than 1,000 people and the Cabinet Office was fined £500,000.

ICO fine – Mermaids Charity

An internal email group was set up without secure settings, leading to confidential and sensitive information being viewable online for three years.

780 pages of confidential emails were affected. The ICO issued a fine of £25,000

3.4 How do you assess "harm" and "damage"?

A personal data breach may lead to physical, material, or non-material damage for the individuals whose data is affected. It may represent one, a combination or all three of these risks.

To assess the type of harm or damage, you can ask the following questions:

Question

✓Have people lost control over their personal information?

✓ Are people at increased risk of identity theft or fraud?

✓ Could people suffer discrimination?

✓ Could people suffer financially?

✓ Could it damage people's reputation?

✓ Could it limit people's ability to exercise their privacy rights?

✓ Is there a breach of confidentiality?

✓ Is there any other disadvantage they could suffer?

Case study – Retail sector

Delivery drivers were given a schedule for deliveries for the day. The paper list was lost by the driver, it is likely it fell on the pavement after a delivery. This list included postal addresses but no names.

Assessment made: This didn't represent significant risk of harm or damage.

Copyright of Data Protection Network. All rights reserved. 2022 ©

Case study – Political membership club

A membership secretary's laptop was stolen from his car. It was not encrypted. The password was not robust. Contents included a list of members, home addresses, email addresses and mobile numbers.

Assessment made: This represented a potential risk of harm and damage to the affected individuals who needed to be informed.

3.5 Rating the risk to affected individuals and the organisation

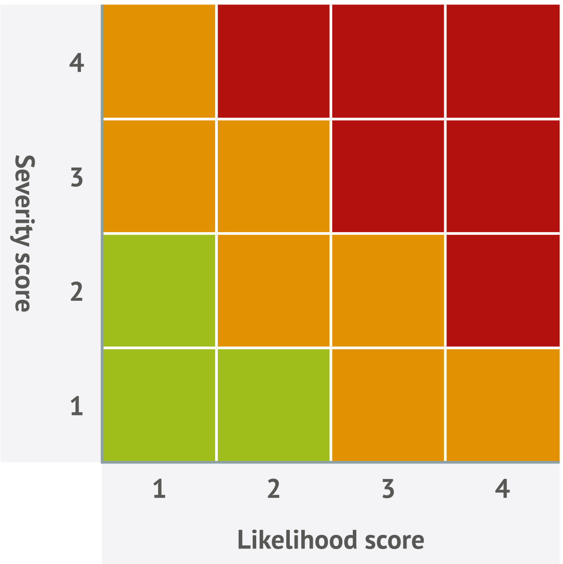
Once you have as much information as possible the risks identified need to be evaluated, balancing the severity of what could happen, with the likelihood of this happening.

The severity could be high, but highly unlikely to happen. Or the severity could be relatively low but highly probable.

It can help to use a risk matrix like the one shown below. This gives you a clear methodology for rating risks and can offer some assurance and evidence your assessment is as objective as possible.

It means you can, for example, score the severity on a scale of low to very high (most severe) and the likelihood from very unlikely to certain.

The example risk matrix below illustrates Red/Amber/Green risk ratings. This is helpful for teams to quickly visualise the scale of each risk. Organisations will take differing approaches to how the rank and colour their risk matrices.



Severity score				
4	🟧	🟥	🟥	🟥
3	🟧	🟧	🟥	🟥
2	🟩	🟧	🟧	🟥
1	🟩	🟩	🟧	🟧
	1	2	3	4
	Likelihood score			

Total risk score = Severity score multiplied by likelihood score (maximum 16)

It's also useful for your leadership team to review these risks and add them to the company risk register (if one is being used).

Copyright of Data Protection Network. All rights reserved. 2022 ©

4. Breach reporting checklists

4.1 Reporting to a Supervisory Authority

The 72-hour clock starts the moment you become 'aware' of a personal data breach. When are you considered to be 'aware'?

- When there's a reasonable degree of certainty a security incident has occurred which might have led to personal data being compromised.
- This may be clear from the outset or may take some time to establish.
- The emphasis is on prompt action to determine whether personal data is involved, and if so, to take remedial action and report if required.

You don't need to have all the facts to report

- A report can be submitted before all the facts are known.
- A full assessment can run in parallel. Any salient information learnt later can be provided as updates, as details emerge and as your risk assessment evolves.
- What might have seemed a significant risk initially, could be downgraded, or vice versa.

How to report

You many need to identify a relevant Supervisory Authority. For UK based organisations this is likely to be the ICO.

The ICO has a '*Report a breach*' online reporting page. There's also an online self-assessment which walks you through the reporting steps.

Reporting checklist

✓ Log the incident

✓ Record all relevant information including risk assessment

✓ Record remedial measures taken

✓ Submit your first report within 72-hours

✓ Update Supervisory Authority as required

Copyright of Data Protection Network. All rights reserved. 2022 ©

4.2 Sector-specific reporting requirements

For certain sectors other laws may apply. In the UK the following sectors have specific reporting requirements.

Health sector: the ICO has a separate notification process for breaches in England and in Wales.

Telecoms and internet service providers: if you are subject to PECR (the Privacy and Electronic Communications Regulations) you should continue to report under PECR - there is no need to report under the DPA 2018 as well.

Communications: certain organisations in the Communications sector have obligations to report to the ICO an incident under the NIS Regulations. NIS applies to two groups of organisations:

- Operators of essential services (OES) - such as energy, transport, health, water and digital infrastructure.
- Relevant digital service providers (RDSPs) - those who provide online marketplaces, online search engines or cloud computing services.

Trust service providers and qualified trust service providers: organisations which provide trust services (including electronic signatures, seals, time stamps, registered delivery services or website authentication certificates) may fall within the eIDAS Regulation. This includes its own data breach obligations and there's a separate notification form for these.

4.3 Informing affected individuals

You need to inform anyone affected by a personal data breach if it's likely to result in a high risk to the rights and freedoms of individuals.

- You must inform them directly and without undue delay.
- You may need to issue a 'holding statement' first, following this up with more information as and when you can.
- Sometimes even if the risk isn't rated as particularly high, people may already be aware, so you may have to communicate with them.

While many organisations may wish to be as open as possible, it's worth considering in cases where there is minimal risk, that telling individuals could cause them unnecessary concern.

Copyright of Data Protection Network. All rights reserved. 2022 ©

Must have in communications to affected individuals

- ✓ A description of what's happened
- ✓ Name and contact details of your DPO (if you have one) or other contact point
- ✓ The likely consequences
- ✓ Measures taken or proposed to handle the incident
- ✓ Measures taken to mitigate any possible adverse effects (where appropriate)

Nice to have (where relevant/possible)

- ✓ Clear and specific advice on steps individuals can take to protect themselves
- ✓ Say what you are willing to do to help them

4.4 When no reporting is required

When you decide the breach does not meet the threshold for reporting to the Supervisory Authority, or informing affected individuals, you should still keep a record of the incident and take steps to avoid similar incidents happening in future, perhaps with worse repercussions.

Checklist for when not reporting

- ✓ Log the breach
- ✓ Implement measures to avoid similar incidents happening again:
    - Remind staff of correct procures
    - Improve security measures
    - Update policies / guidelines
    - Raise awareness
- ✓ Record justification for not reporting

Copyright of Data Protection Network. All rights reserved. 2022 ©

5. How technology can help

5.1 Preventing a breach

Technology has a big part to play in maintaining the confidentiality, integrity and availability of personal data, right from the very moment data is first acquired by the business.

Rigorous information security measures and controls can help to prevent a data breach happening in the first place – or at least reduce the severity when it occurs. Measures like encrypting mobile devices, multi-factor authentication, network security controls, automated monitoring & detection tools… the list goes on.

> *In reality, it is not a matter of if, but when. Plan that it will happen.*
> **Ray Pathak, Vice President Data Privacy, Exterro**

ICO fine – British Airways

An attack on BA's systems exposed personal data and credit card information in a 2018 breach. The ICO investigation found that numerous measures could have been deployed to prevent this happening in the first place.

The breach affected 400,000 customers and staff. The ICO issued a fine of £20 million.

It's vital to make sure you have effective back-up and recovery routines in case the worst happens.

For businesses using platforms like Microsoft 365 or Google Workspace, your Administrator will have an array of security tools at their disposal to protect the data, so it can pay to take a closer look at the tools you're already paying for.

As Martin Turner, Managing Director, Full Frame Technology says:

> *Technology can play a crucial role in helping to prevent a data breach, and in dealing with the aftermath if one happens. But technology is not a panacea; it has to work hand in hand with effective governance. And it's almost always worth checking that existing solutions are being used to their full potential.*

Copyright of Data Protection Network. All rights reserved. 2022 ©

5.2 Cyber Essentials certification

Cyber Essentials is a government-backed scheme designed to help organisations assess their readiness and protect themselves against cyber threats, whilst demonstrating your commitment to cyber security.

Certification or self-certification includes many basic cyber security measures such as patching, back-ups and two-factor/multi-factor authentication.

5.3 Security incident management & investigation

Detecting cyber incidents and attacks is not easy, but technology can help by looking out for warning signs. Triggers can indicate that a security incident or breach is occurring. For example, suspicious network activity, changes to infrastructure, changes to system accounts and passwords, and so on.

When a data incident is detected on your systems, or reported by individuals, having the right technology and support in place means you can respond more quickly and decisively.

Fortunately, the technology available to support with data breaches has evolved enormously in recent years, often but not always, powered by advancements in computing power and AI.

Digital forensic tools can help you diagnose exactly what's occurred, if personal or sensitive data is involved and who has been affected. It can help you identify the types of processing affected, how your employees and business partners may be affected, and if a bad actor is involved.

5.4 Breach assessment tools

Some privacy management solutions include data breach assessment modules which will help you to gather the information you need, conduct a robust assessment, score the risks, and keep appropriate records.

These tools help streamline the process of managing a breach, by providing automated workflows and templates to assist the investigation, assessment and remediation.

We also see privacy management technology used to maintain Records of Processing Activities (RoPAs). These records can prove useful if you suffer a breach – helping you quickly 'join up the dots' to know exactly what processing may be affected and which stakeholders need to be involved in mitigating any adverse impact.

> “*Technology is key to a timely, secure and defensible response to managing a breach. From making the process more efficient, to allowing for secure communication and uploading of evidence to providing single source of truth audit record. With the proliferation of breaches today, organisations can ill afford not having technology in their breach response process.*”
>
> **Ray Pathak, Vice President Data Privacy, Exterro**

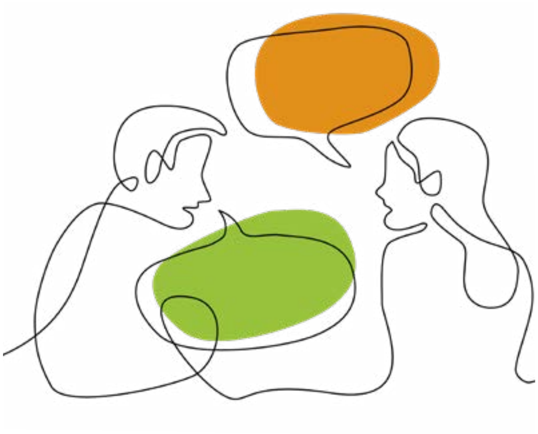
Copyright of Data Protection Network. All rights reserved. 2022 ©

DPN

About DPN

Data Protection Network (DPN) publishes expert analysis, insight and resources. Our content is written and developed by a team of data protection specialists, members of our Advisory Group and other respected contributors.

In 2017 the DPN published the first definitive industry guidance on legitimate interests and in 2020 we published detailed data retention guidance. In 2022, the DPN has published its inaugural Privacy Pulse Report to test the temperature of the data protection and privacy community.



The DPN also runs regular webinars where DPOs and other privacy professionals share their experiences and practical tips.

How we can help?

Our experienced team provide no-nonsense privacy advice and support, across a range of sectors. Our goal is to make data protection relevant and easy to understand. Based on extensive real-world experience, our team continues to stay at the forefront of data protection. To learn more about us visit: *dpnetwork.org.uk*.

Copyright of Data Protection Network. All rights reserved. 2022 ©

About Exterro

Exterro empowers the world's largest organisations, law firms and Government agencies to proactively and defensibly manage their Legal Governance, Risk and Compliance (Legal GRC) requirements.

Exterro's Legal GRC software is the only comprehensive platform that automates the complex interconnections of data privacy, legal operations, digital forensics, and cybersecurity compliance. Thousands of legal teams, IT leaders and investigators around the world trust our integrated Legal GRC platform to manage their risks and drive successful outcomes at a lower cost. For more information, visit *www.exterro.com*.

Exterro Privacy Software

Quickly and easily identify, map, manage and protect your organisation's data to establish robust global privacy compliance processes.

Exterro provides the most effective and defensible way to accurately develop and maintain a comprehensive data inventory. Combined with the ability to efficiently leverage data and records retention rules that address legal and business requirements while reducing risks and costs, you'll be in safe hands with the world's most trusted software solutions for meeting domestic and international regulatory obligations.

Back to contents ◁

Copyright of Data Protection Network. All rights reserved. 2022 ©

Appendix – Useful resources

Resource	Link
ICO Ransomware Guidance	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/
ICO Personal Data Breach Guidance	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
ICO Data Breach Guidance for Small Businesses	https://ico.org.uk/for-organisations/sme-web-hub/72-hours-how-to-respond-to-a-personal-data-breach/
EU Guidelines on Personal Data Breach Notification	https://ec.europa.eu/newsroom/article29/items/612052
EU Guidelines on Examples regarding Personal Data Breach Notification	https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en
EU Agency for Cybersecurity (ENISA) Recommendations for a methodology of the assessment of severity of personal data breaches	https://www.enisa.europa.eu/publications/dbn-severity

Copyright of Data Protection Network. All rights reserved. 2022 ©

Copyright of Data Protection Network. All rights reserved. 2022 ©

www.dpnetwork.org.uk

DATA PROTECTION NETWORK