GDPR

DATA BREACH SURVIVAL GUIDE

Your quick reference checklist to preparing for the inevitable

harrison clark rickerbys
SOLICITORS

SUFFERED A DATA BREACH?

This is what to do

Whether you've emailed the wrong recipient or you've suffered a cyber-attack, if you've experienced a data breach of any nature, you must take action.

First things first, don't panic.

But once you're over the initial shock of realising that 'something bad has happened', taking a swift and proportionate response is a must. This survival guide shows you how to structure your data breach response plan and provides practical advice on the action you must take.

How to assess a data breach

= 0-24 hours

Report what's happened to your breach response team, Data Protection Officer, or Data Protection Manager, so that they can determine the severity of the breach. They will assess the situation and seek answers to the following questions:

- Has there actually been a breach and is personal data involved?
- Has control of the data been lost?
- When was the breach discovered (time and date)?
- What type of data has been affected?
- How many records are concerned?
- Can the breach be rectified immediately? If so, rectify it – but still record it.
- Who needs to know?

Your organisation should have clear lines of reporting for a data breach.

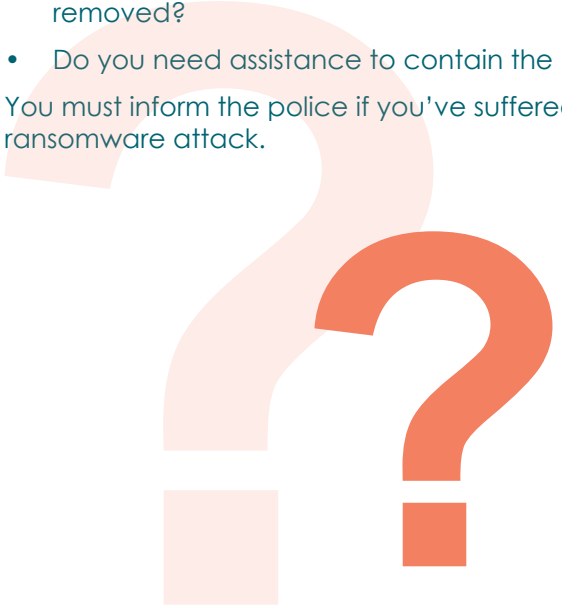
How to contain a data breach

Not every breach will be the same. Once the seriousness of the breach has been assessed you should deploy the most appropriate containment strategy, for example, from simply needing to recall an email, to disconnecting entirely from the internet.

Key questions to ask are:

- What led to the breach and can that cause be removed?
- Do you need assistance to contain the breach?

You must inform the police if you've suffered a ransomware attack.



Should you report to the ICO?

= 48-72 hours

Not all breaches have to be **reported**, but all breaches should be **recorded**. Open your survival guide for our ICO notification flow chart.

When recording and reporting, you must note:

- The nature of the personal data breach – i.e. the details of the breach and approximate number of people affected, including if they are children or vulnerable people
- The likely consequences of the personal data breach
- The measures proposed or taken to address the personal data breach and mitigate its possible adverse effects.

Confirm to the ICO who they should contact for more information.

PREVENTION IS BETTER THAN CURE

We recommend you follow best practice by putting together a data breach response team, so that when a breach happens you are ready.

Your data breach response team may include:

- Team leader
- Project manager
- Senior member of staff with overall accountability for privacy (this may be your Data Protection Officer or Manager)
- Legal support
- Risk management support
- IT support to help establish the cause and impact of any data breach that involves ICT systems
- Information and records management expertise to assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and to provide advice on recording the response to the data breach
- Human resources
- Media/ communications expertise.

Have the phone numbers (including 'out of hours') of your data breach response team easily at hand. Have these printed out in case the breach causes your systems to go down.

Be clear on roles and responsibilities and allocate the following tasks:

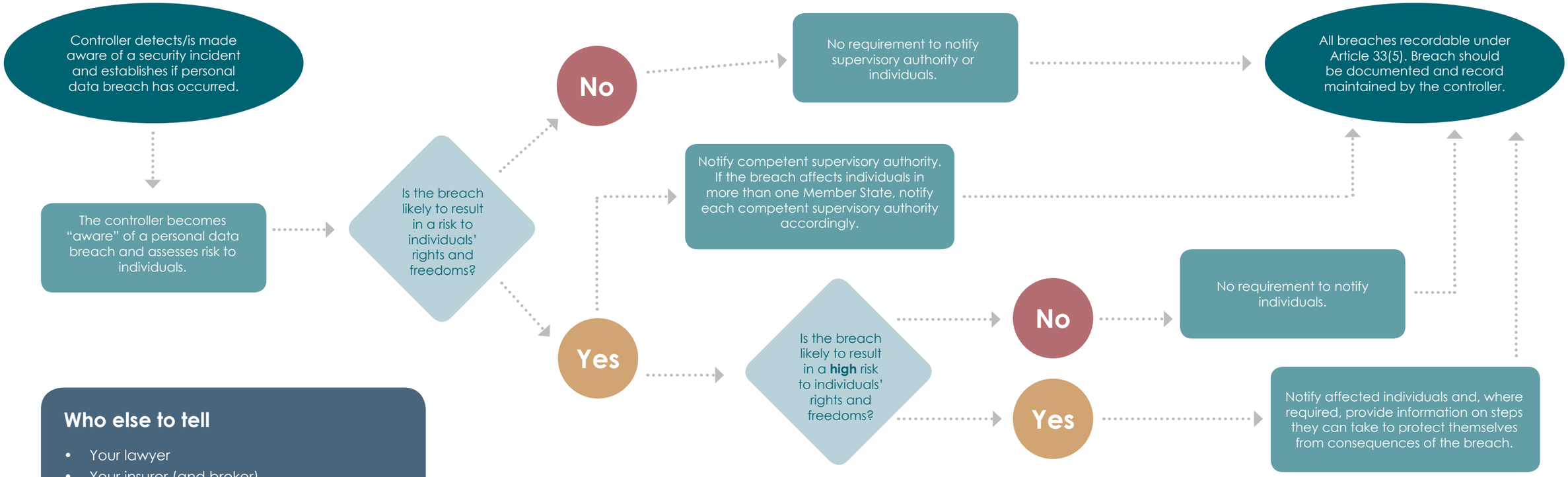
- Assessing the breach
- Controlling communications about the breach to customers, stakeholders, regulators and law enforcement
- Devising and implementing potential strategies for containing and remedying the breach.

Know your business

The data breach response team should be familiar with and have tested other recovery plans which might be relevant, such as the Disaster Recovery Plan, Incident Response Plan and the Business Continuity Plan.

GDPR NOTIFICATION REQUIREMENTS PROCESS

How to manage a data breach



Source: European Commission's 'Article 29 Data Protection Working Party'

Who else to tell

- Your lawyer
- Your insurer (and broker)
- The police
- Your customers and other stakeholders.

TOP TIPS FOR SURVIVAL

1 Write a data breach response plan and put your breach response team in place.

2 Make sure your staff are trained to understand their obligations and how to spot a data breach.

3 Ensure your policies are up to date and designed to work with each other.

4 Test your response and recovery plans at least annually.

5 Learn from your mistakes. Review and amend your approach if you suffer a breach.

6 Talk to us. Our GDPR expert advisors are on-hand to help you – whether that is with prevention or cure.

Call us on 01905 744 814

harrison clark rickerbys
SOLICITORS

Talk to us

Our GDPR expert advisors are on-hand to help you – whether that is with prevention or cure.

Call us on

01905 744 814

www.hcrlaw.com