Data Privacy Advisory Service

An Introduction to Managing a Data Breach

Use this to help your team deal with data breaches

Introduction

In recent years, the number of personal data breaches has increased significantly due to several factors including the Covid-19 Pandemic. Data breaches are categorized based on the likelihood of the breach's impact on the rights and freedoms of data subjects. Moreover, data breaches can also have significant consequences for the data controllers and processors.
For example, companies can receive enforcement action or fines from the ICO. These fines can be up to £17.5 million or 4% of annual global turnover – whichever is greater – for infringements such as data breaches.
Therefore, it is critical that your organisation is compliant. Below, we have outlined some steps on how to ensure your organisation is compliant with the reporting and management of data breaches.

Training: Are your staff adequately trained?

Many data breaches happen because the individuals involved did not understand the consequences of a data breach or understand fully what personal data is. Early identification of a data breach and ensuring staff's understanding of personal data is fundamental to good compliance. The legal definition of personal data, as per GDPR, is under Article 4 (1). Additionally, ensuring that all staff complete their data protection training on a regular basis (an annual basis is recommended), will help improve staff awareness and understanding of data breaches. More specifically role-based training is recommended so staff can understand the risks associated with personal data in real-world situations.

Reporting Process: Are your staff aware of this process?

Staff should be the front-line response in data breach management. Many delays in the reporting of data breaches occur because staff did not know how to report a data breach to the information governance or data protection team within their organisation.

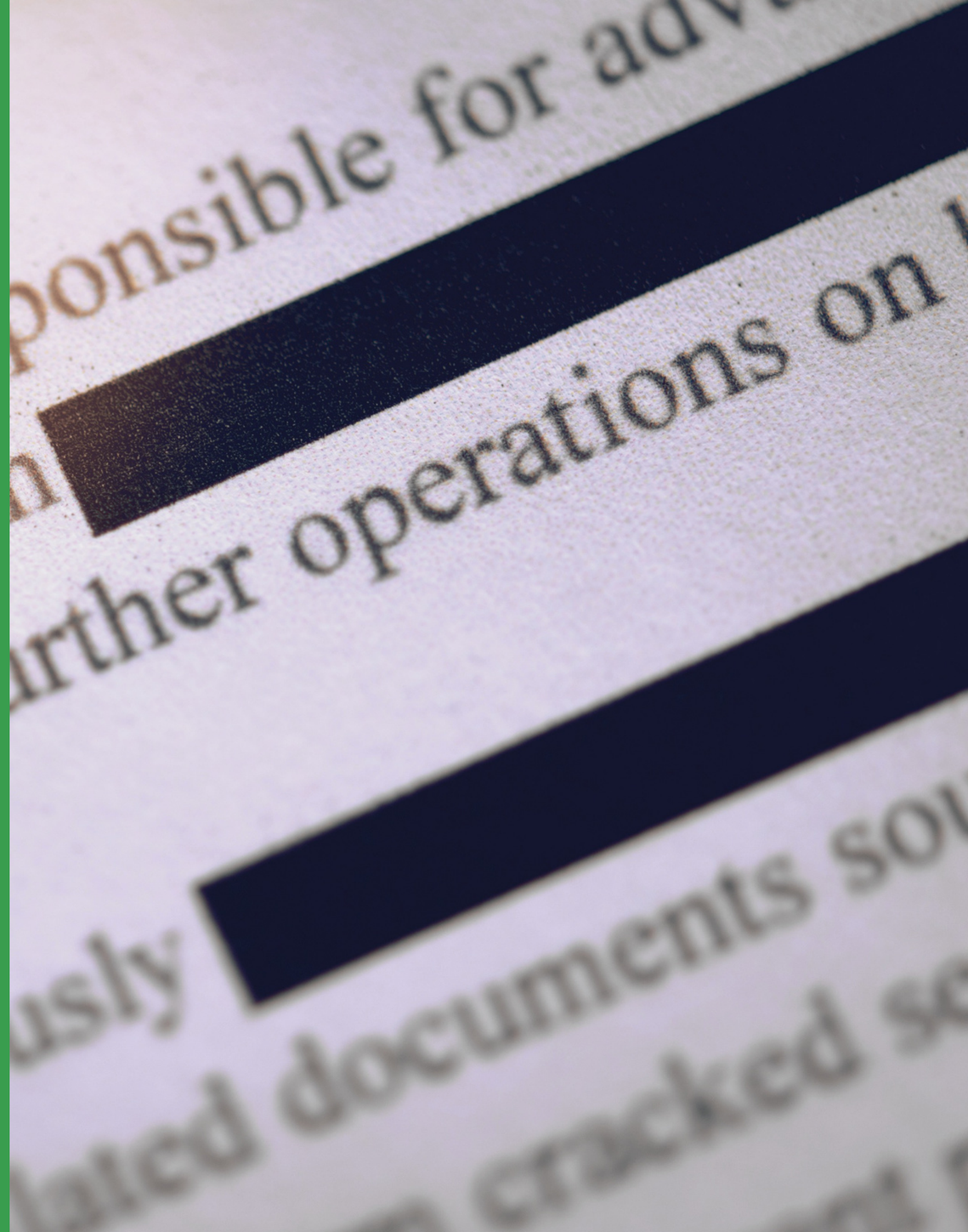
Therefore, it is key to establish a clear reporting process, that is easy to follow and understand. It is also recommended that an incident report template be made available to all staff so they can collect as much information about the data breach as soon as possible as part of the reporting process. This will improve your organisation’s compliance with data breach reporting.

Containment and Recovery of Data: Are your staff aware of this process?

Containing each data breach and recovering the affected personal data is just as important as reporting the breach to the data protection team and thus the ICO if appropriate. As such staff should know what to do in the event of a data breach. If an email was sent in error by Egress or Outlook, staff should know how to revoke or recall emails.

It is recommended that user guides on how to contain breaches should be distributed to all staff on how to use these functions along with other scenarios.

What do I share with the ICO?



Under section 67 of GDPR controllers must notify the ICO without undue delay and where feasible no later than 72 hours after being made aware of the personal data breach. However, the ICO recommends that you only report high-risk breaches, where there was a significant risk to the data subject's rights and freedoms.

Despite this, it is still key to document every data breach to demonstrate compliance as well as use these reports to identify any trends in data breaches within your organisation. If you are still investigating the data breach, article 33 (4) of GDPR allows you to report the information relating to the data breach to the ICO in phases, if this is done without any further unnecessary delays.

Do I need to notify the affected data subject(s)?

Only data subjects who have had a significant risk to their rights and freedoms warrant notification of the data breach without undue delay according to GDPR.

Controllers must inform the affected data subjects of the facts relating to the breach, its effects and any remedial action taken.

Prevention is Key

Prevention is just as important as knowing how to effectively manage a data breach. There are many methods on how to mitigate the risks of a data breach some of which we have outlined below.

Policies and Processes: Are they robust enough?

Every organisation should have data protection and personal information security policies in place to ensure that staff are aware of their data protection responsibilities. Furthermore, these policies should be supported by effective processes in mitigating the risks of a data breach.

It is also recommended that organisations regularly review these policies and processes to ensure that they are robust and in line with current best practices in the industry. Process failure is another common cause of data breaches, reinforcing the need for regularly reviewing existing processes.

Staff Awareness of Official Policies and Procedures

Clarifying the expectations that employers have, will help remind employees of what the appropriate guidelines are to follow when safeguarding personal data and ensures everyone is on the same page.

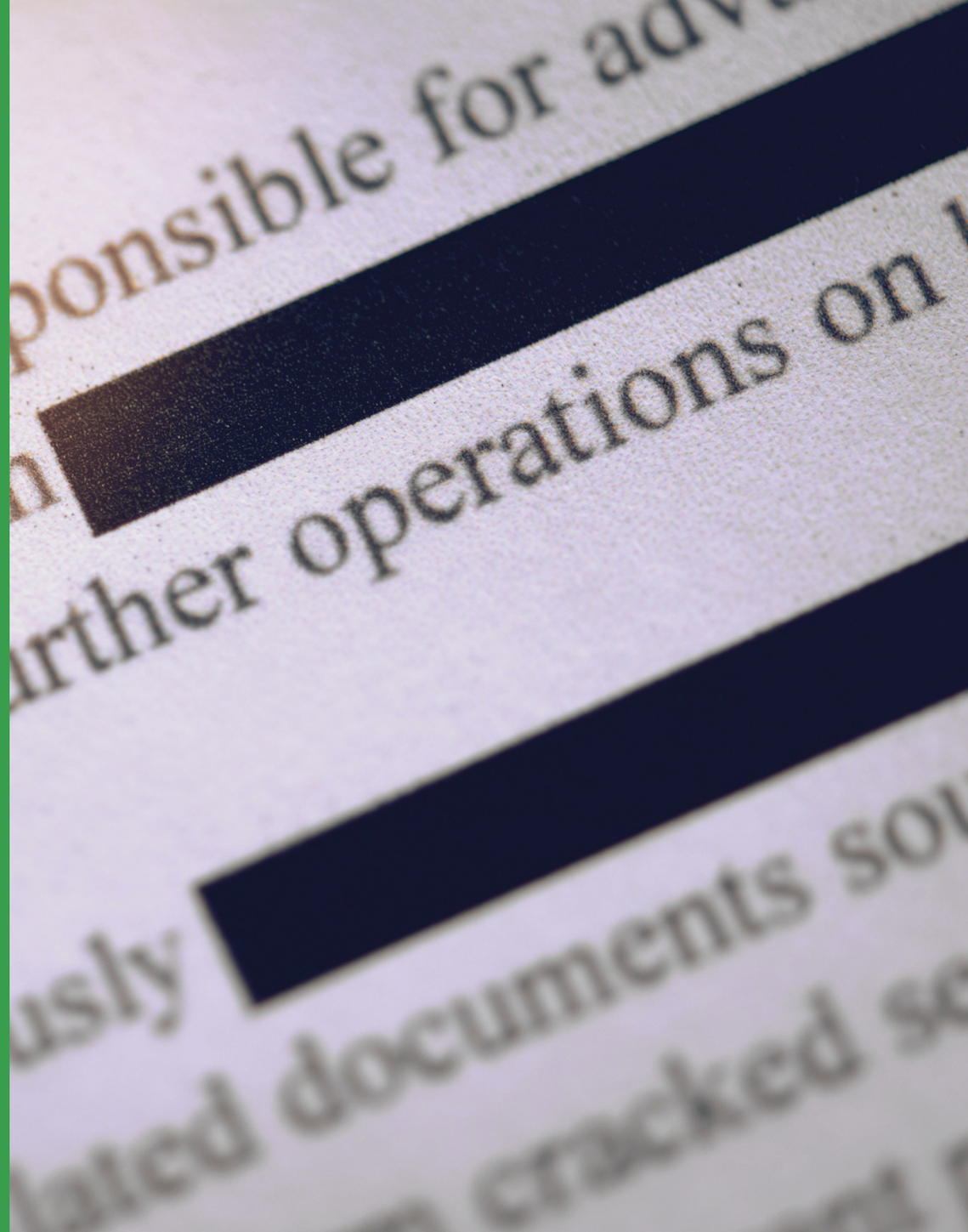
These policies and procedures are only effective if they are appropriately communicated across the organisation.

Security Awareness

Regularly reminding employees of the best practices with respect to data protection and cyber security will ensure that your organisation is best equipped to prevent data breaches.

Staff should be regularly reminded to keep their operating systems, and software on their devices up to date. To support this, staff should regularly check their devices for viruses and other security threats by using the approved anti-virus software.

Layers of Security



To prevent unauthorised access, organisations should regularly update their security protocols notably password security. The National Cyber Security Centre recommends that everyone should use a three-word passphrase instead of a password as part of their #thinkrandom campaign.

Furthermore, staff should be regularly educated on the best cyber security practices and should be reminded not to open unverified links or attachments as well as to never use unapproved software for communication and data sharing. Multi-factor authentication should also be considered as another layer of security to prevent unauthorised access to devices and accounts.

Keeping Vigilant

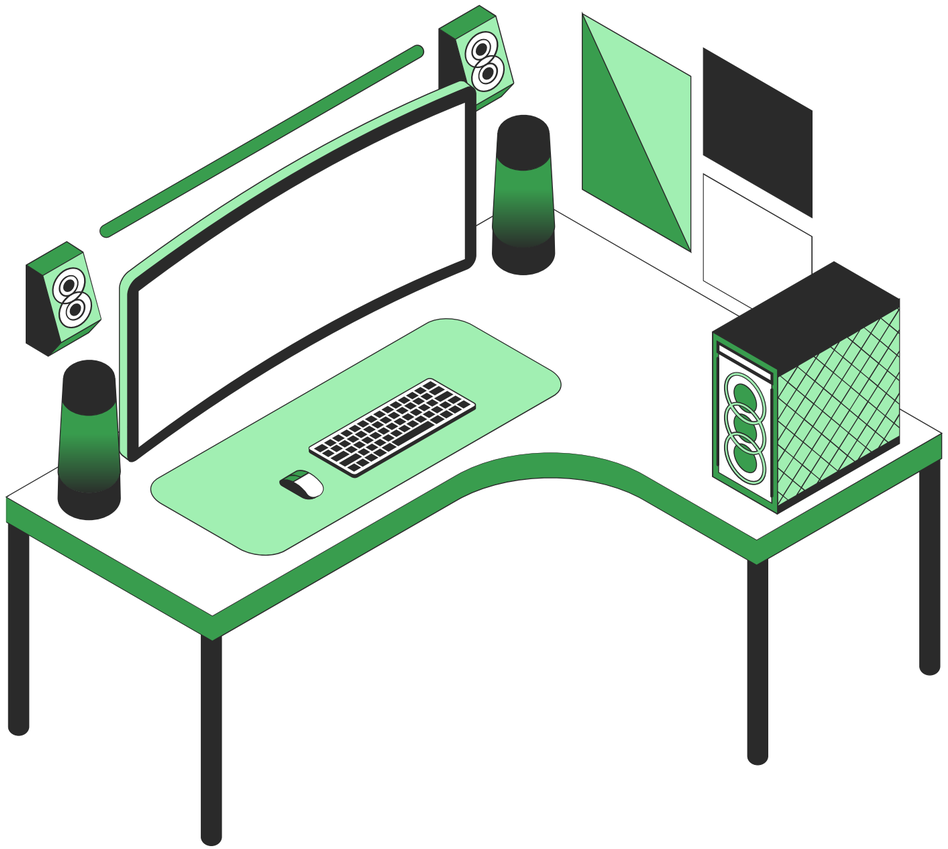
Many data breaches are caused by human error because staff are distracted or stressed. Staff should be encouraged to break up tasks into manageable chunks where they can completely focus on each task and not get distracted by other pieces of work.

This will also mitigate the risk of data breaches as staff will become more vigilant and check everything before they share personal data.

Data Protection Checklist

It is recommended that organisations should create a data protection checklist to act as a visual prompt to remind staff of the importance of due diligence.

The implementation of data protection checklists for tasks also helps remind team members to slow down and focus on one task at a time. Adapting the data protection checklists for each team provides an opportunity for staff to share solutions to common mistakes so the team can learn from each other’s mistakes.



Do you have any questions?

Data breach management can seem like an insurmountable task, but DPAS can help you develop effective strategies on how to prevent and manage data breaches. For further information get in touch with the DPAS team.

www.dataprivacyadvisory.com
info@dataprivacyadvisory.com