RISK SOLUTIONS

Presented by RS Risk Solutions Ltd

CHECKLIST | PERSONAL DATA BREACHES UNDER THE GDPR

The General Data Protection Regulation (GDPR) introduced a duty on all organisations to report certain types of personal data breaches to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

A personal data breach refers to a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

In 2018, 43 per cent of all UK organisations experienced at least one cyber-security breach or attack, according to the government's cyber-security breaches survey.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must inform those individuals without undue delay. You should ensure that you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals. You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

Under the GDPR, an organisation may be fined up to €20 million (roughly £16 million) or 4 per cent of its annual turnover—whichever is higher—for violating the basic principles related to data security. What's more, if your organisation fails to notify the relevant supervisory authority of a breach, it can result in a fine of up to €10 million or 2 per cent of your annual turnover, depending on which is higher.

Use this checklist to comply with the GDPR's rules surrounding personal data breaches:

PREPARING FOR A DATA BREACH	YES	NO	ADDITIONAL NOTES
We know how to recognise a personal data breach.	☐	☐	
We understand that a personal data breach isn't only about loss or theft of personal data.	☐	☐	
We have prepared a response plan for addressing any personal data breaches that occur.	☐	☐	
We have allocated responsibility for managing breaches to a dedicated person or team.	☐	☐	
Our staff knows how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.	☐	☐	

RESPONDING TO A DATA BREACH	YES	NO	ADDITIONAL NOTES
We have in place a process to assess the likely risk to individuals as a result of a breach.	☐	☐	
We know who is the relevant supervisory authority for our processing activities.	☐	☐	
We have a process to notify the Information Commissioner's Office (ICO) of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.	☐	☐	
We know what information we must give the ICO about a breach.	☐	☐	
We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.	☐	☐	
We know we must inform affected individuals without undue delay.	☐	☐	
We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.	☐	☐	
We document all breaches, even if they don't all need to be reported.	☐	☐	

HOW TO REPORT A DATA BREACH	COMPLETED
Contact the relevant supervisory authority of a breach within 72 hours of your organisation becoming aware of it.	☐
Directly contact individuals affected by a breach if it is likely to result in a high risk to their rights and freedoms. (Note: A 'high risk' means the threshold for notifying individuals is greater than notifying the relevant supervisory authority.)	☐
Complete a breach notification, which should contain the following information: • The categories and number of individuals affected by the breach • The categories and number of personal data records affected by the breach • The name and contact details of the data protection officer (if your organisation has one) or an additional contact where more information can be obtained • A detailed description of the potential consequences of the data breach • A detailed description of what measures your organisation has taken or will take to address the data breach • A detailed description of the measures your organisation has taken or will take to mitigate any possible adverse effects to either itself or the individuals affected	☐

NOTIFICATION REQUIREMENTS OF A PERSONAL DATA BREACH: