GDPR

Personal data breaches checklist

ADLANTIC

Intro

The General Data Protection Regulation (GDPR) determines how your business does business from 25 May 2018.

Your business will need to manage, administer and protect personal data whether you work in B2B or B2C marketing.

According to a 2017 IAPP survey, the number one overall riskiest obligation organizations are worried about comply with is preparing for and handling data breaches.

Contents

1. At a glance
2. Preparing for a data breach
3. Responding to a personal data breach
4. How do we notify a breach to the ICO?
5. About

This checklist is a guide for **personal data breaches** only. Please note it is a living document and the ICO is working towards expanding key areas of the GDPR itself.

The ICO has a checklist for both data controllers and data processors here.

Credit to the Information Commissioner's Office (ICO) GDPR consent guidance: www.ico.org.uk

ADLANTIC

At a glance

What is a data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

At a glance

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority.
- **You must do this within 72 hours of becoming aware of the breach, where feasible.**
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure 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.

1 Preparing

Preparing for a personal data breach

- ☐ 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 know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

2 Responding

Responding to a personal data breach

- ☐ 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 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.

Reporting a breach

How do we notify a breach to the ICO?

To notify the ICO of a personal data breach, please see the ICO pages on reporting a breach. Summary details for reporting below:

Call the ICO on, 0303 123 1113

What information will I need to provide?

When you phone, the ICO will ask you:

- what has happened;
- when and how you found out about the breach;
- the people that have been or may be affected by the breach;
- what you are doing as a result of the breach; and who we should contact if we need more information and who else you have told.

The ICO will send you a copy of the information you give this.

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority.

This means that as part of your breach response plan, you should establish which European data protection agency would be your lead supervisory authority for the processing activities that have been subject to the breach.

About

Adlantic® is a digital marketing services and training company based in Glasgow and London.

Our mission is to help global marketers put people first with consent based marketing.

Events

1. GDPR 1 - May
2. GDPR 2 - Late May
3. GDPR 3 - June

Data Protection Services

1. Audit
2. Review & Validation
3. Implementation
4. Virtual DPO
5. Privacy Management

Checklist Sources:
Credit to the Information Commissioner's Office (ICO) GDPR consent guidance: www.ico.org.uk

ADLANTIC