Data Breach Notification Form

# Document Purpose

This document forms part of the GDPR toolkit which has been created in partnership with Black Penny Consulting. The GDPR toolkit is a self-service guide for alignment to the GDPR.

The GDPR Breach Notification Form is a template that can be used to manage the process of incident breach.

# Introduction

The organisation must make sure that all personal data breaches are reported to the Trustee Board in a timely manner. The only instance where reporting may not be necessary is when the personal data breach is unlikely to result in risking the rights and freedoms of the subject.

# Responsibilities

The Trustee Board is responsible for making sure that responses are complete and timely.

All adult volunteers who interact with data subjects are responsible for making sure that a personal data breach is reported to the Trustee Board, and that they provide as much detail as possible.

# Reporting a data breach to the supervisory authority

The Trustee Board may need to report to the [Information Commissioner’s Office](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) (ICO) within 72 hours after becoming aware of a personal data breach, if it meets a certain criticality A separate ICO form is required for this available on the ICO website.

The notification referred to in paragraph one shall at least:

* describe the nature of the personal data breach
* outline the categories and approximate number of data subjects concerned
* outline the categories and approximate number of personal data records concerned
* communicate the name and contact details of the Trustee Board
* describe the likely consequences of the personal data breach
* describe the measures taken or proposed to be taken by the Trustee Board to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Please complete the form below and pass it to the Trustee Board as soon as a breach has been detected. In addition this form should passed to The Scout Association via the following email address dpa.alert@scouts.org.uk. NOTE – This email address is only for reporting a breach and there will be no remediation guidance as a direct result. The information will be used to monitor any trends in breaches being reported and update the Scout Unit Data Protection Toolkit with further guidance.

A breach can be:

* the disclosure of confidential data to unauthorised individuals
* the loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data e.g. PCs, USBs, mobile phones, laptops, disks etc
* the loss or theft of paper records
* inappropriate access controls allowing unauthorised use of information
* a suspected breach of the business’s IT security and acceptable use policies
* attempts to gain unauthorised access to computer systems, e.g. hacking
* records altered or deleted without authorisation from the data ‘owner’
* viruses or other security attacks on IT equipment systems or networks
* breaches of physical security for example forcing of doors or windows into a secure room or filing cabinet containing confidential information
* confidential information left unlocked in accessible areas
* insecure disposal of confidential paper waste
* leaving IT equipment unattended when logged in to a user account without locking the screen to stop others accessing information
* the publication of confidential data on the internet in error and accidental disclosure of passwords
* misdirected emails or faxes containing identifiable personal, confidential or sensitive data

# Breach response template

|  |  |
| --- | --- |
| **NAME** **ADDRESS** |  |
| **Trustee Board Details** |  |

**Notice of personal data breach**

|  |  |
| --- | --- |
| **Date of breach** |  |
| **Breach description** |  |
| **Breach effect** |  |
| **Number of data subjects affected** |  |
| **Personal data affected** |  |
| **Number of personal data records affected** |  |
| **Likely consequences of the breach** |  |
| **Remedial action taken** |  |
| **Have data subjects been notified and justification** |  |
| **Date of remediation**  |  |

|  |  |
| --- | --- |
| **SIGNED** |  |
| **NAME AND TITLE** |  |

**Data Breach Severity**

When assessing the severity of a data breach, some of the things you may wish to consider are:

* The IT systems, equipment, devices, records involved in the security breach
* What is the nature of the information lost?
* How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?
* Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the organisation or third parties?
* How many data subjects are affected?
* Is the data bound by any contractual security arrangements?
* What is the nature of the sensitivity of the data?
* Whether it includes any HIGH RISK DATA such as:
	+ Sensitive personal data (as defined in the Data Protection Act) relating to a living, identifiable individual’s
		- racial or ethnic origin
		- political opinions or religious or philosophical beliefs
		- membership of a trade union
		- physical or mental health or condition or sexual life
		- commission or alleged commission of any offence, or
		- proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings
	+ Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as National Insurance Number and copies of passports and visas
	+ Personal information relating to vulnerable adults and children
	+ Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed
	+ Security information that would compromise the safety of individuals if disclosed

|  |  |
| --- | --- |
| **Action taken** | **To be completed by the Trustee Board** |
| **Incident number** | **e.g. DB/year/001** |
| **Report received by:** |  |
| **On (date):** |  |
| **Action taken by responsible officer/s:** |  |
| **Was incident reported to police?** | **Yes/No** **If YES, notified on (date):** |
| **Follow up action required/recommended:** |  |
| **Reported to the Trustee Board on (date):** |  |
| **Reported to other internal stakeholders (details, dates):** |  |
| **For use of the Trustee Board** |  |
| **Notification to ICO** | **YES/NO If YES, notified on:****Details:** |
| **Notification to data subjects** | **YES/NO If YES, notified on:****Details:** |
| **Notification to other external, regulator/stakeholder** | **YES/NO If YES, notified on:****Details:** |