The GDPR toolkit

GDPR Breach Notification Form

Version 2.1 - June 2020

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Reason for change** |
| 1.0 | 23/03/2018 | Baseline |
| 1.1 | 10/05/2018 | Added requirement to notify TSA of a breach by passing the breach notification form |
| 2.1 | 18/05/2020 | Rebrand |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[Document Purpose 3](#_Toc509561875)

[Introduction 3](#_Toc509561876)

[Responsibilities 3](#_Toc509561877)

[Reporting a data breach to the supervisory authority 3](#_Toc509561878)

[Breach response template 5](#_Toc509561879)

# 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 Executive Committee 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 Executive Committee 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 Executive Committee, and that they provide as much detail as possible.

# Reporting a data breach to the supervisory authority

The Executive Committee 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.

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 Executive Committee
* describe the likely consequences of the personal data breach
* describe the measures taken or proposed to be taken by the Executive Committee 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 Executive Committee 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](mailto:dpa.alert@scouts.org.uk?subject=Data%20Breach%20Notification). 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 GDPR 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** |  |
| **Executive Committee 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** |  |
| **Date of remediation** |  |

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