Cognisco Ltd

Breach Notification to Data Controller Procedure

Document Ref:	(Ref)
Version:	1
Date of version:	06/02/2018
Author:	A Ellis
Approved by:	(Approver)
Confidentiality level:	Public / Internal / Confidential [Delete as appropriate]

Amendment History

Date	Version	Author	Details of Amendment
(Date)	1	(Author)	Initial Release

Scope

This procedure applies in the event of a personal data breach under Article 33 Notification of a personal data breach to the supervisory authority, and Article 34 Communication of a personal data breach to the data subject of the GDPR.

The GDPR draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. Therefore, each organisation, should establish whether it is data controller, or a data processor for the same data processing activity; it must be one or the other.

Responsibilities

All users (whether Employees/Staff, contractors or temporary Employees/Staff and third-party users) and [owners] of Cognisco Ltd are required to be aware of, and to follow this procedure in the event of a personal data breach.

Procedure- Breach Notification Data processor to Data Controller

- Cognisco Ltd shall report any personal data breach to the data controller without undue delay by phone with a follow up email [if you process data for a number of controllers, where is this information specified?].
- The (Data Protection Officer / GDPR Owner) / [Relationship owner] notifies their contact within the data controller, which is recorded in the PIMS19 Internal Breach Register.
- Notification is made by [email, phone call, etc.].
- Confirmation of receipt of this information is made by [email, phone call, etc.].

- Procedure – Breach Notification Data Controller to Supervisory Authority
- Cognisco Ltd shall notify the supervisory authority ICO without undue delay, of a personal data breach.
- Cognisco Ltd assesses whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.
- If a risk to the data subject is likely, Cognisco Ltd shall report any personal data breach to the supervisory authority without undue delay, and where feasible not later than 72 hours. Where data breach notification to the supervisory authority is not made within 72 hours, it shall be accompanied by the reasons for the delay.
- The data controller shall provide the following information to the supervisory authority (PIMS20. Breach Notification Form):
    - 4.4
    - 4.4.1 A description of the nature of the breach
    - 4.4.2 The categories of personal data affected
    - 4.4.3 Approximate number of data subjects affected
    - 4.4.4 Approximate number of personal data records affected
    - 4.4.5 Name and contact details of the (Data Protection Officer / GDPR Owner) / (Relationship Owner)
    - 4.4.6 Likely consequences of the breach
    - 4.4.7 Any measures that have been or will be taken to address the breach, including mitigation
    - 4.4.8 The information relating to the data breach, which may be provided in phases.
- The (Data Protection Officer / GDPR Owner) / (Relationship Owner) notifies their contact within the supervisory authority, which is recorded in PIMS19. Internal Breach Register.
- Notification is made by [email, phone call, etc.].
- Confirmation of receipt of this information is made by [email, phone call, etc.].

Procedure – Breach Notification Data Controller to Data Subject

- Where the personal data breach is likely to result in high risk to the rights and freedoms of the data subject Cognisco Ltd shall notify the affected data subjects without undue delay, [using this form/in accordance with the (Data Protection Officer / GDPR Owner) / (Relationship Owner)'s recommendations].
- The notification to the data subject shall describe in clear and plain language the nature of the breach including the information specified 4.4 above.
- Appropriate measures have been taken to render the personal data unusable to any person who is not authorised to access it, such as encryption.
- The data controller has taken subsequent measure to ensure that the rights and freedoms of the data subjects are no longer likely to materialise.

- Where it would require a disproportionate amount of effort to identify and contact the data subject directly, there shall be a public communication or similar measure whereby the data subject is informed in an equally effective manner.
- The supervisory authority may, where it considers the likelihood of a personal data breach resulting in high risk, require the data controller to communicate the personal data breach to the data subject.

Document Management

This document is valid as of January 2018.

This document is reviewed periodically and at least annually to ensure compliance with the following prescribed criteria.

- General Data Protection Regulation
- Legislative requirements defined by law, where appropriate

(Role)
(Author)

_____
(Signature)