Colleague

Data Breach Policy

1. Overview

Any data breach can have major consequences both for the company and the individuals whose information could be compromised. Colleague Software takes great measures to prevent data breaches and if they do occur then the data is highly encrypted.

2. Purpose

The purpose of this policy is to establish a high standard for how Colleague Software responds to a data breach. It also ensures full disclosure to any individuals who could have had their personal information compromised.

3. Scope

The scope of this policy includes all Colleague Software employees.

4. Policy

Data breach examples:

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

4.1 Detection

4.1.1 Any individual who suspects that a theft, breach or exposure of personal or sensitive data must immediately report and provide a description to either a company director or the Data Protection Officer.

4.1.2 The data protection officer is responsible for putting in to place data audits to detect possible data breaches. This audit must be monitored at a set interval.

4.1.3 It is the responsibility of the Data Protection Officer to assess and report the extent and possible impact of the data breach, this must include what data has been potentially exposed.

4.2 GDPR notification to ICO

4.2.1 The Data Protection Officer must determine the impact of the data breach to individuals. If this could result in a risk to people's rights and freedoms. Then you must follow the below steps in 4.2.x

4.2.2 The Data Protection Officer or company director must inform the ICO with 72 hours of discovering the breach, even if all the details are not yet known. This can be done via: https://ico.org.uk/for-organisations/report-a-breach/

4.2.3 The report to ICO must include:

- A description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned; and
  - The categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

4.3 Response

4.3.1 The Data Protection Officer must chair a meeting with the company directors and any other employees with information of the breach.

4.3.2 The meeting must determine if there is high risk to individuals whose personal data has been exposed because of the breach.

4.3.3 If a high risk is determined then the individuals must be informed, see 4.4

4.3.4 Explanation on how the breach occurred and of any failures by processes, employees or IT systems were to blame must be reported.

4.3.5 Details on how to prevent similar breaches must be raised and acted on.

4.4 Notifying Individuals

4.4.1 If it has been determined in step 4.3.2 that there is a high risk to individuals the they must be notified.

4.4.2 The following information must be provided:

- description, in clear and plain language, the nature of the personal data breach and, at least:
  - the name and contact details of the data protection officer or other contact point where more information can be obtained;
  - a description of the likely consequences of the personal data breach; and
  - a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

4.5 Recording

4.5.1 It is the responsibility of the Data Protection Officer to record all data breaches, even if the risk is very low.

5. Policy Compliance

5.1 Compliance Measurement

It is the responsibility of the Data Protection Officer to ensure this policy in complied to.

5.2 Exceptions

Any exception to the policy must be approved by a company director in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Information

- ICO: https://ico.org.uk/for-organisations/

Last Update Status: Updated April 2018

Colleague

7 Revision History

Date of Change	Responsible	Summary of Change
April 2018	Trevor Etherington	Policy created

Last Update Status: Updated April 2018