MSS-DP DOC 11.4

Data Breach Reporting

Procedure

Retirement Capital

Version 1.0 June 2020

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification:** | Company Confidential | | |
| **Version:** | 1.0 | | |
| **Document title:** | MSS-DP DOC 11.4 | | |
| **Document management** | Gavin McCloskey | **Authorised by:** | Gavin McCloskey |
| **Revision interval:** | Annually/ad hoc | **Last revision:** | 14/11/2020 |

Contents

[Revision History 2](#_Toc8208628)

[1. Management Summary 4](#_Toc8208629)

[2. Data Breach 4](#_Toc8208630)

[3. Data Breach Reporting 4](#_Toc8208631)

[3.1. Initial escalation 4](#_Toc8208632)

[3.2. Assessment 4](#_Toc8208633)

[3.3. ICO and customer notification 4](#_Toc8208634)

[3.4. Details for reporting a breach 5](#_Toc8208635)

[4. Review 5](#_Toc8208636)

# Management Summary

Retirement Capital operates in compliance with the Data Protection Act 2018, the UK implementation of the European General Data Protection Regulations. As such we will evaluate any suspected data breach to determine its nature and risk to the business and to personal information. As required by the Act, any applicable breaches will be reported to the Information Commissioners Office.

# Data Breach

Any form of actual or suspected data breach must be reported immediately to the Data Protection Officer. A data breach could be, but is not limited to, one of the following:

* Spear Phishing emails
* Loss of company memory stick
* Perceived overheard conversations or overlooked computer screen
* Loss of phone, tablet, laptop or other computing equipment
* Loss of confidential paperwork or files
* Loss or corruption of any records
* Supplier data breach
* Customer reported data breach
* Concerns over loss or misuse of personal data

# Data Breach Reporting

## Initial escalation

Any suspected data breach must be reported immediately to the Data Protection Officer (DPO) by email to

**If in any doubt, report the incident** – issues of this type occur but sometimes only become a serious issue if not reported and risks mitigated.

## Assessment

The DPO will investigate the nature of the breach to:

* determine if there is a potential risk to personal information;
* mitigate risks;
* to prevent further breaches

## ICO and customer notification

The DPO will determine if the breach needs to be reported to the Information Commissioner’s Office or customers, suppliers or affected individuals and will take the necessary action following conversations with the ICO and customer’s DPO.

The ICO must be notified within 24 hours of identifying a breach.

## Details for reporting a breach

* Registration Number: XXX-XXX
* ICO contact details: 01494 493 535
* Further details: [www.ico.org.uk/for-organisations/report-a-breach/](http://www.ico.org.uk/for-organisations/report-a-breach/)

# Review

This policy will be reviewed annually and from time to time to ensure that it remains consistent with UK regulations and recommendations.