DATA BREACH ESCALATION AND EXTERNAL REPORTING PROCESS

The Information Commissioner's guidance on data breach reporting and Ordnance Survey's process for external reporting.

OFFICIAL

Responsibility for this document

[redacted] is responsible for the content of this document.

Change history

Version	Date	Summary of change
1.0	Nov 2015	First issue

The impacts of the policy, described in this document have been assessed and where appropriate, changed, in accordance with the requirements set out in Ordnance Survey's Equality scheme.

As a requirement of Ordnance Survey's Equality scheme all of our processes and activities, including all policies, projects and proposals, must be screened to assess any impact with regard to race, disability and gender equality.

Please ensure that this document has been equality screened and include the above statement, only when this has been completed, with the brackets removed. You must notify your Equality Advocate who will ensure that all necessary records are updated. Your Equality Advocate can also help you with the screening process, if required.

Distribution

This document is for use by Ordnance Survey staff. The document, or any part of it, **must not** be supplied or communicated to any other individual or organisation without the prior written permission of the owner.

Trademarks

Contents

1. INTRODUCTION

Ordnance Survey and its group of companies (known as OS Group) are committed to complying with legislation and Government mandated requirements in the protection and security of our business information. OS recognises that data handling will never be entirely risk free, therefore, as well as policies, processes and technologies in place to minimise data loss, we should also make provision to minimise the negative impact of any incident should they occur and provide a process for the escalation reporting of any breaches.

2. INFORMATION COMMISSIONERS GUIDANCE FOR REPORTING DATA BREACHES

The seventh principle of the Data Protection Act says

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office. The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the DPA.

'Serious breaches' are not defined. However, the following should assist OS Group in its role as a data controller, in considering whether breaches should be reported:

2. 1 The potential detriment to the individuals such as exposure to identity theft through the release of non-public information about their private life. Detriment includes emotional distress as well as both physical and financial damage.

2. 2 The volume of personal data that is lost/released/corrupted and the likelihood of individuals suffering some harm.

2. 3 The sensitivity of the data lost/released/corrupted. Even where smaller amounts of personal data are involved, the release could cause significant risk or distress to the individual. This is most likely to be the case for sensitive personal data.

Examples of reportable data breaches (not an exhaustive list)

Detriment to individuals: Any data loss that runs the risk of causing emotional distress as well as both physical and financial damage, such as financial information, personnel records, or customers being able to see the information and order history of another customer.
Volume of Data: Theft or loss of an unencrypted laptop or other portable media holding names, addresses, dates of birth, national insurance numbers of 100 individuals or a full customer database copied to an unencrypted personal laptop.
Sensitivity of Data The loss of a paper filing system or unencrypted device holding information on trade union membership, health conditions, race or ethnic origin.

3. ESCALATION PROCESS

[redacted] will take the lead in containing and investigating the data breach. This will result in an incident investigation report detailing the background to the incident, remedial actions and recommendations going forward.

[redacted] will inform [redacted] and the Business Group Director of the nature of the data breach on the same day it is identified.

[redacted] and the Business Group Director will be advised of the proposal to report to the ICO.

As a result of the investigation and with the opinion of [redacted], if the data breach meets any of the criteria listed in Section 2 above, the Information Commissioners Office will be advised of the data loss. This will be actioned by [redacted], following the guidance on the ICO's website. https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

All data breach incidents will be investigated by [redacted] and recorded on the Data Protection Act Breach Register GEN\12\14282.