Esh Group

General Data Protection Regulation (GDPR)

Dealing with a Data Protection Breach

Version	Date
1st Draft	11 May 2018
Next review date – 25 November 2018	

Introduction

The General Data Protection Regulation 2018 re-emphasises earlier legislation regarding the need to report Data Protection Breaches. In general, any breach needs to be reported to the Information Commissioners Office (ICO) within 72 hours of being aware of the breach.

What is a breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A breach is likely to result in an elevated risk of adversely affecting individuals' rights and freedoms. A breach is often thought of as personal data being lost or stolen but there are many more possibilities where a breach can occur e.g. someone could inadvertently or deliberately disclose data by sending to the wrong customer or supplier, or data could be accessed by an unauthorised third party.

Where personal data has been encrypted then there is no need to report a breach externally, however the breach should still be reported internally by advising Mark Sowerby, Esh Group Data Protection Officer (for contact details see the 'Where to go for further guidance' section below) who will arrange the incident to be logged with reasons for non-reporting.

Our policy - who to report the breach to and when

Note that how to report the breach is covered in the next section below.

- We will inform the ICO within 72 hours of becoming aware of the breach.
- We will inform any appropriate external relevant partners as they often require notification within the 72-hour timeframe e.g. where we may handle/process personal data on behalf of a framework partner/major client.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.
- All breaches should first be notified to Mark Sowerby, Esh Group Data Protection Officer (for contact details see the 'Where to go for further guidance' section below).

How to report the breach

- Where an employee becomes aware of a possible data breach then they should immediately notify Mark Sowerby or Don McMenzie (for contact details see the 'Where to go for further guidance' section below) and they will form a 'Response Team' as appropriate – you may be requested to be part of this team.

- The Response team is also likely to include the relevant Business MD, the Head of IT and a representative from Group marketing.

- The Response Team will investigate and confirm whether a breach has occurred or otherwise.

- Where a breach has been established the 'Response Team' will set about containing the breach thus preventing any further breach.

- The Response team will confirm who to report this to including the ICO and, where appropriate, any partner where Esh is the data processor on behalf of that partner (breach reporting requirements may well be stipulated in a Contract Addendum/Data Sharing Agreement with the partner).

- In reporting a breach, you need to 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 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.

- All communication with the ICO will be made through Mark Sowerby, or should he be unavailable, The Head of Group Compliance.

- The preferred method of reporting is normally to call the ICO helpline on 0303 123 1113. Details of the telephone conversation need to be documented. There is also an online reporting option with the ICO that can be used where we are sure that we have dealt with the breach appropriately.

- For the method of reporting to partners, this will be driven by Contract Addendum/Data Sharing Agreement with the partner, and in conjunction with the relevant Business MD.

- Any necessary communication with individuals affected by the breach will be authorised by the Response Team. The method of reporting to individuals will be addressed on the merits of the circumstances around the breach.

Where to go for further guidance

- Internal contacts

  Mark Sowerby, Chief Financial Officer (Esh Group Data Protection Officer)

  T: 0191 377 4500

  DD: 0191 377 4183

  M: 07771 973969

  Email: mark.sowerby@esh.uk.com

  Don McMenzie, Internal Auditor

  T: 0191 377 4500 (no direct dial)

  M: 07773 4719

  Email : don.mcmenzie@esh.uk.com

- Information Commissioners Office

  https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/