Data breach notification procedure

For The Holistic Group Limited
23.05.18

1.0 Introduction

The Holistic Group Limited, a company incorporated in England & Wales (registration number: 4792134) whose registered office and trading address is at 24 Southwark Bridge Road, London SE1 9HF ("the Company"), has a range of measures in place in order to protect the personal data that we hold. Despite our best endeavours, it is possible that a situation will occur where our data protection measures are breached. The purpose of this document is to set out the approach that the Company will take should this situation arise.

Our data breach and notification procedure is one element of how we fulfil our obligations under the General Data Protection Regulation 2016 ("GDPR").

The following policies and procedures also support the Company with ensuring GDPR compliance:

- Privacy statement
- Record retention and protection policy
- Data subject access request procedure

2.0 General principles

The Company has some clear requirements when it comes to reporting serious incidents which relate to personal data and which may impact the rights and freedoms of data subjects. These are:

- it must report any serious breach to the Information Commissioners Office (ICO) as soon as possible but within 72 hours of the Company becoming aware of the issue.
- where a breach occurs, we must inform data subjects without undue delay.

3.0 The requirement to report the breach

It is important to note that the requirement to report a breach to either the ICO or to the data subject depends on the severity of the breach. The breach only needs to be reported if the breach represents a risk to the rights of the data subject. The Company will assess any breach which occurs and will decide on the relevant reporting requirements based on the level of risk we believe exists.

The information that will be taken into consideration when assessing the breach is:

- whether the personal data was encrypted
- if encrypted, the strength of the encryption used
- to what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- the data items included e.g. name, address, bank details, biometrics
- the volume of data involved
- the number of data subjects affected
- the nature of the breach e.g. theft, accidental destruction
- any other factors that are deemed to be relevant

The risk assessment will be undertaken by the Managing Director and Office Manager and the reasons for the decision need to be clearly documented.

Even if a data breach is not deemed to have been significant enough to warrant reporting to either the ICO or the data subject, it will be recorded in our data breach register.

4.0 Notifying the ICO

Where it is deemed that a breach needs to be reported to the ICO then it is the responsibility of the Managing Director and Office Manager to complete this activity. The Managing Director and Office Manger are aware of this requirement and know the process that needs to be followed.

5.0 Notifying data subjects

Where it is deemed that a breach needs to be reported to data subjects then it is the responsibility of the Managing Director and Office Manager to complete this activity. The Managing Director and Office Manager are aware of this requirement and know the process that needs to be followed.

Data subjects will be informed of:

- the nature of the breach
- whether the breach has been reported to the ICO
- what measures have been taken to mitigate the risk to data subjects
- what actions if any, will be taken to minimise the risk of a similar breach occurring in the future

6.0 Concerns and questions

GDPR is new legislation and how the rules are interpreted will continue to evolve. The Company will continue to adopt best endeavours to ensure our on-going compliance but any individual who has concerns regarding any of the actions that we are taking or feels that they are unclear as to how the Company is complying with elements of the legislation should raise their concerns with the Office Manager. Your concerns will be investigated and responded to within 28 days.