OCRA (LONDON) LIMITED

Data Breach Policy

OCRA (LONDON) LIMITED
3RD Floor
14 Hanover Street
London
W1S 1YH
United Kingdom
T : 0207 317 0600
F: 0207 317 0610
E privacy@ocra.co.uk
www.ocra.co.uk

Contents

1 Interpretation

1.1 The definitions provided in the Company's Data Protection Policy apply equally to this Data Breach Policy.

2 About this Policy

2.1 The Company recognises the need to have in place a robust process for responding to any suspected or reported Data Breach to ensure that it can act quickly and efficiently to protect data (particularly Personal Data) and mitigate against the potential damage which the breach may cause.

2.2 This Policy sets out the Company's approach and processes in the event of a Personal Data Breach and should be read in conjunction with the Company's Data Protection Policy and other Privacy Policies.

2.3 This Data Breach Policy applies to all Company Personnel. All Company Personnel must read, understand and comply with this Data Breach Policy and the Company's Privacy Policies when Processing Personal Data on the Company's behalf and attend training provided on its requirements.

2.4 Any breach of this Data Breach Policy or other Privacy Policy may result in disciplinary action.

2.5 This Policy does not form part of any Contract between the Company and Company Personnel or the Company and any other third party (including clients, customers and agents).

3 What is a Personal Data Breach?

3.1 A Personal Data Breach is any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Company or its third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach.

3.2 Personal Data Breaches may occur unintentionally, accidentally or intentionally and can arise in a number of different ways, for example:

3.2.1 loss or theft of data or equipment on which data is stored (such as a laptop, USB stick or a document);

3.2.2 unauthorised use, alteration or disclosure of data;

3.2.3 human error (for example, accidentally sending an e-mail or a letter to the wrong recipient);

3.2.4 a cyber-attack;

3.2.5 unauthorised access to the Company's IT system (including malicious viruses and links in spam e-mails, known as "blagging" offences);

3.2.6 other unforeseeable incidents such as equipment failure, fire or flood;

3.2.7 loss of availability or destruction of personal data

4 Internal Reporting

4.1 If you discover, suspect or receive any report of a Personal Data Breach, you should contact your line manager or the DPM immediately. The Company only has 72 hours to assess the Data Breach and report it to the Information Commissioner's Office (the **ICO**), if required. If your line manager or the DPM is unavailable, you should contact a member of the Board of Directors.

5 Initial Risk Assessment

5.1 The DPM will carry out an assessment of risk and determine the seriousness or potential seriousness of the Data Breach, having regard to the following assessment criteria:

5.1.1 the type of the breach;

5.1.2 the nature, sensitivity and volume of Personal Data (having regard to other Personal Data which may be available about the Data Subject);

5.1.3 the ease of identification of individuals (including whether identification could be possible with no special research needed);

5.1.4 the severity of consequences for the individual (in particular, whether there is risk of identity theft, fraud, physical harm, psychological distress, humiliation or damage to reputation);

5.1.5 special characteristics of the Data Subjects and whether this may affect the level of impact of the breach on them;

5.1.6 the number of Data Subjects affected; and

5.1.7 any other considerations deemed necessary or appropriate.

5.2 It is recognised that some Data Breaches will not be serious Data Breaches, for example, where a laptop is irreparably damaged but its files are backed up and can be recovered. However, it is necessary to carry out a risk assessment on each reported Data Breach in order to ensure that the risks are understood and properly addressed.

6 Containment and Recovery

6.1 The DPM, together with other senior Managers (e.g. the IT Manager, HR Manager, Marketing Manager, and external consultants (the Containment Team)) will be responsible for taking further steps which are necessary to mitigate and limit the potential damage of any Personal Data Breach in accordance with this Policy.

6.2 The Containment Team will:

6.2.1 analyse the nature of the Data Breach;

6.2.2 establish whether there is anything which can be done to mitigate and/or recover any losses and limit the damage that the breach has caused or could potentially cause;

6.2.3 take appropriate steps to minimise the effect of the breach (if it is ongoing);

6.2.4 establish which parties need to be notified (both internally and externally) in accordance with Clause 7 of this policy;

6.2.5 establish whether there is any illegal activity which should be reported to the police or any other appropriate authorities;

6.2.6 establish whether there has been any breach of any confidentiality obligations which the Company owes to any third parties.

6.3 The Containment Team will decide which steps are appropriate, will be responsible for the assessment of ongoing risk, prepare a risk assessment in order to assess the scale of the data breach and the potential losses arising out of it, and carry out ongoing assessments of risk at regular intervals as may be appropriate.

6.4 The Containment Team will keep a written copy of the risk assessment, and will update it with any developments, the outcome of its investigation and attempts to contain the Data Breach.

6.5 The DPM is responsible for ensuring that all recommendations of the Containment Team are implemented.

7 Recording and notifying the Data Breach

Recording the Personal Data Breach

7.1 Regardless of whether the Company is required, or deems it necessary, to notify the Data Breach to the ICO, the DPM will record in the Company's Data Processing Record-all breaches notified to or identified by the DPM.

7.2 Records will include the facts relating to the Data Breach, its effects and any remedial action taken (if necessary).

Notifying the Personal Data Breach to the ICO

7.3 The DPM will consider whether it is appropriate to notify the ICO of the Data Breach. The Company's approach is that it is appropriate in all circumstances to notify the ICO of a Data Breach, except where the Data Breach is unlikely to result in a material risk to the rights and freedoms of Data Subjects.

7.4 A material risk to the rights and freedoms of Data Subjects will include risks of discrimination, identity theft of fraud, financial loss, damage to reputation or confidentiality.

7.5 The DPM shall ensure that it notifies the ICO of any relevant Data Breach within 72 hours after becoming aware of the breach.

7.6 The DPM will normally notify the ICO by using the ICO's standard format to determine the nature of the information which needs to be provided.

7.7 Where it is not possible to provide all of the information which the ICO requires at the time of notification, the DPM may provide the information in phases in order to avoid delays in the initial notification. As soon as further information becomes available, the DPM will provide this to the ICO without undue further delay.

7.8 In addition to the information set out above, any notification to the ICO shall also include:

7.8.1 where possible, the categories and approximate number of Data Subjects affected or involved and number of records concerned;

7.8.2 a description of the likely consequences of the breach;

7.8.3 the DPM's contact details.

Notifying the Personal Data Breach to the Data Subject

7.9 The DPM will notify the Data Subject affected by the Data Breach where the Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subject.

It is recognised that the threshold for notifying the Data Subject is higher than the threshold for notifying the ICO and that not all breaches will therefore require to be communicated to Data Subjects.

7.10 If it is necessary to notify a Data Subject, the DPM will do so as soon as is reasonably feasible. The DPM will also liaise with the ICO (or any other appropriate supervisory authority and the Company's advisors) to seek advice about the nature of the information to be provided to the Data Subjects.

7.11 Any notification made to Data Subjects should include (to the extent appropriate):

7.11.1 sufficient details of the nature of the Data Breach (including when and how it happened);

7.11.2 what Personal Data was or could possibly be involved;

7.11.3 what steps the Company has already taken and will take to mitigate the risks;

7.11.4 where appropriate, what steps the Data Subject can take to mitigate the risks (for example, notifying their banks or obtaining a free credit report);

7.11.5 how the Data Subject can contact the Company to discuss the Data Breach.

7.12 In the event of any doubt about notification obligations or the contents of any notices, the DPM will seek legal advice in respect of the same.

8 Evaluation and Response

8.1 The DPM will consider whether the Data Breach was as the result of any failings (for example, lack of adequate security, unclear allocation of roles and responsibilities) or inadequate user protocols and will consider whether there is a need for additional security and control requirements in relation to the handling of Personal Data and, if so, how the Company can put these processes in place.

8.2 The DPM will also consider whether there is a need for additional training of Company Personnel having regard to whether Company Personnel need to be made aware of how to mitigate and be vigilant against Data Breaches.

9 Changes to this policy

9.1 The Company reserves the right to change this Data Breach Policy at any time without notice. It is your responsibility to ensure that your knowledge of this Data Breach Policy is up to date and that you comply with its terms.