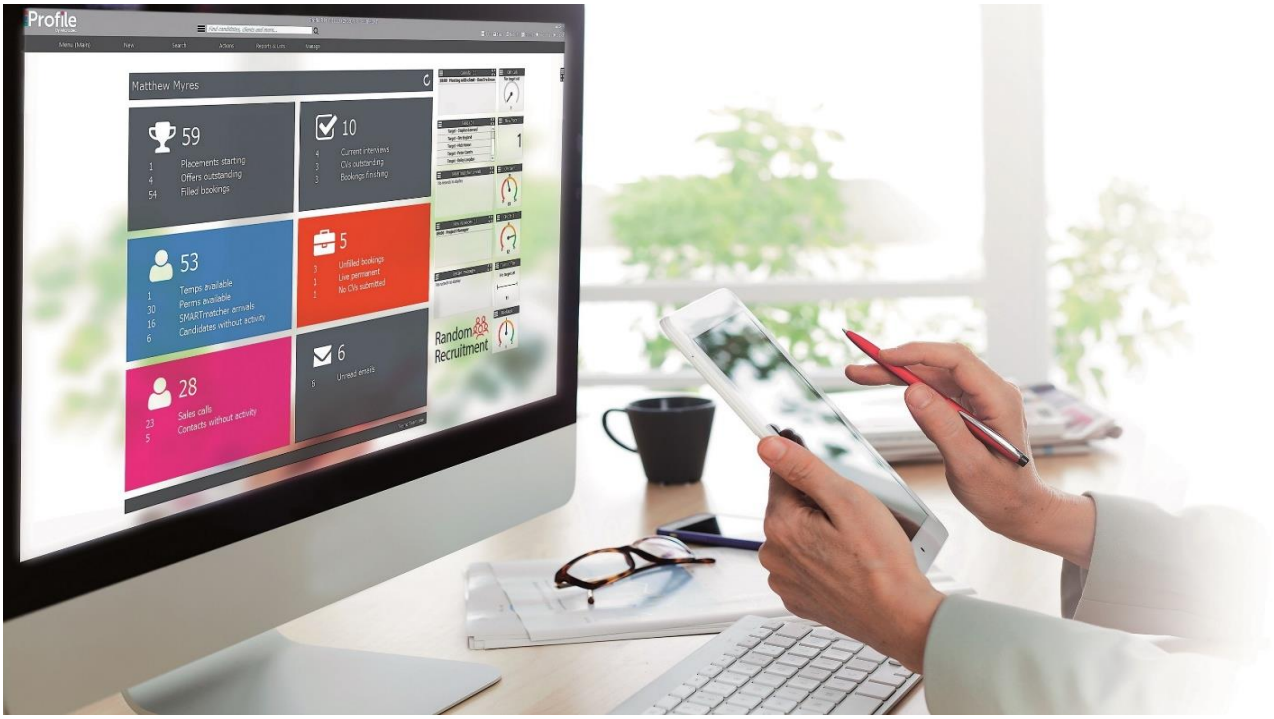
DATA BREACH NOTIFICATION POLICY

Details how we will manage a data breach and notify our clients and the authorities



DATA BREACH NOTIFICATION POLICY

Author	Linda Clark
Document Title	Data Breach Policy
Date Last Updated	01/02/2018 17:21
Date of Next Review	
Document Path	M:\Microdec\HR\Policies and Procedures\Data-Breach-Notification-Policy.docx
Pages	7
Copyright	Unauthorised publication or distribution is prohibited. All Right Reserved Copyright Microdec © 2018
Security Classification	Public

Revisions Table

Version	Reviewed by	Date	Sections Changed?
1.00		12/01/2018	First Version

Table of Contents

1. Purpose

Microdec holds and processes personal data on behalf of its staff and clients, a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a security breach that could compromise data. Compromise of information, confidentiality, integrity, or availability may result in harm to individuals, reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs including significant fines from the Information Commissioner's Office (ICO).

The company is obliged under the Data Protection Act to have in place systems designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

The GDPR makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals. Processors must notify any breach to their controllers. Controllers and processors are therefore encouraged to put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals, and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary.

2. Scope

This Policy relates to all personal and sensitive data controlled or processed by the company regardless of format.

This Policy applies to all employees, contractors, consultants, temporary staff, and other workers at Microdec and data processors working for, or on behalf of the company.

2.1. Types of Personal Data Breaches

2.1.1. Confidentiality breach

Where there is an unauthorised or accidental disclosure of, or access to, personal data.

For Example:

- personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it;
- client database being compromised, for example being accessed by another client;
- paper records containing personal data being left unprotected for anyone to see, for example: files left out when the owner is away from their desk and at the end of the day, papers not properly disposed of in confidential shredding bins, papers left at printers;
- staff accessing or disclosing personal data outside the requirements or authorisation of their job;
- being deceived by a third party into improperly releasing the personal data of another person;

2.1.2. Availability breach

Where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

For Example:

- loss or theft of laptops, mobile devices, or paper records containing personal data;
- the loss of personal data due to unforeseen circumstances such as a fire or flood;

- when there has been a permanent loss of, or destruction of, personal data;

2.1.3. Integrity breach

Where there is an unauthorised or accidental alteration of personal data.

For Example:

- The removal or false alteration of individuals' mobile numbers or email addresses

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, availability and integrity of personal data at the same time, as well as any combination of these.

3. Policy

On discovery of a data breach the following actions should be taken:-

- Containment and recovery
- Assessing the risk
- Notification of breach to the Information Commissioner's Office (ICO)
- Evaluation and response.

3.1. Containment and Recovery

The individual committing the breach or having identified a possible breach should immediately inform their manager or the Information Security Officer.

The immediate priority is to contain the breach and limit its scope and impact.

- Where personal data has been seen, accessed or been sent to someone who does not have a legitimate need to see it, staff should contact the recipient and
  - tell the recipient not to pass it on or discuss it with anyone else;
  - tell the recipient to destroy or delete the personal data they have received and get them to confirm in writing that they have done so;
  - warn the recipient of any implications if they further disclose the data
- Where data has been lost, altered or has become unavailable, then access to the data should be resumed as quickly as possible via backup copies of the data if necessary.
- Where the data controller is a Microdec client, the client's Data Protection Officer or person responsible for receiving breach notifications is to be given an initial notification stating what recovery processes are being performed with further information about the breach provided in phases as information becomes available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

A Breach Notification incident should be logged on the Internal IT Support system (see the Information Security Incident Logging Policy) stating:

1. date and time of the breach;
2. date and time breach detected;
3. who committed the breach;

4. details of the breach;
5. number of data subjects involved (an approximation is sufficient);
6. details of actions already taken in relation to the containment and recovery.

3.2. Assessing the Risk

The Information Security Officer or Data Protection Officer or a nominated person will conduct an investigation into the breach and prepare a Breach Report.

This report will follow the ICO's guidance on Breach Management and will consider the following:

1. How the breach occurred.
2. The type of personal data involved.
3. The number of data subjects affected by the breach.
4. Who the data subjects are.
5. The sensitivity of the data breached.
6. What harm to the data subjects can arise? For example, the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation
7. What could happen if the personal data is used inappropriately or illegally?
8. For personal data that has been lost or stolen, are there any protections in place such as encryption?
9. The measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects
10. Whether the breach should be notified to the ICO – if NOT the reasoning behind this decision including reasons why the breach is unlikely to result in a risk to the rights and freedoms of individuals

3.3. Breach notification

3.3.1. To the Information Commissioner's Office (ICO)

Under Article 33 of the GDPR - In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The Data Protection Officer or information Security Officer or in the absence of either of these people, any member of the Senior Leadership Team, will determine whether the breach is one which is required to be notified to the ICO.

NOTE: Where the data breach involves any client data either hosted by Microdec or remotely accessed by Microdec staff the responsibility for reporting the breach is with the controller(s) ie. The clients' Data Protection Officers or person responsible for breach notifications.

When notifying a breach to the ICO include the Breach Report with the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

3.3.2. To the affected individuals

If a breach is also assessed to be likely to result in a **high risk** to the rights and freedoms of individuals, the individuals themselves must be informed directly and without undue delay, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

When informing the individuals the following needs to be supplied in clear and plain language:

1. the nature of the personal data breach,
2. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
3. a description of the likely consequences of the personal data breach; and
4. a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

3.4. Evaluation and response

Once the breach has been dealt with the cause of the breach needs to be considered. There may be a need to update policies and procedures, or to conduct additional training.

Head office, UK
Jupiter House
Warley Hill Business Park
The Drive, Brentwood
Essex CM13 3BE
•
+44(0) 1277 227778

Sydney, Australia
Level 34, AMP Centre
50 Bridge Street
Sydney
NSW, 2000
•
+61(2) 8216 0772

Manchester, UK
Stafford Court
145 Washway Road
Sale, Cheshire
M33 7PE
•
+44(0) 161 8711044