Multimatic	**Multimatic Data Breach Reporting Policy (EU and UK)**	**Rev: 03**
	Document Type: **POLICY** / PROCESS / GUIDELINE / OTHER	
	Approved by: Kim Silvestri (Vice President & General Counsel)	
	Author: Kevin Florey (Senior Human Resources Manager - UK)	
	Oversight Responsibility: Senior Human Resources Manager - UK	
	Original Enactment Date: May 23, 2018	Languages: English only
	Current Version Date: November 1, 2023	Shared via: Corporate website, Multimatic CFT website, MultiNET (SharePoint)
	Next Review Date: TBD	Classification: Public

Multimatic Data Breach Reporting Policy

In compliance with the EU General Data Protection Regulation and the UK General Data Protection Regulation

*For the purpose of this Policy, "Multimatic" means each of Multimatic Ltd. (UK), Multimatic U.K. Limited, Multimatic CFT Limited (UK), MTCE Limited (UK), Multimatic Marketing & Service Centre GmbH (Germany), Multimatic Engineering Prague s.r.o. (Czech Republic) and their respective divisions, branches and offices. To the extent any personal data is shared with the Multimatic Corporate Office (Multimatic Inc. (Canada)), reference to Multimatic will also include Multimatic Inc.

TABLE OF CONTENTS

ENGLISH VERSION

*Multimatic Data Breach Reporting Policy

The protection of personal data is important to *Multimatic.

We collect and process information about individuals (personal data) for business purposes, including employment and HR administration, provision of our goods and services, marketing and business administration. This includes personal data relating to our employees, customers, suppliers and other third parties.

Compliance with data protection law is essential to ensure that personal data remains safe, our business operations are secure and the rights of individuals are respected. Reasonable and proportionate care is taken to protect personal data to avoid a data protection breach (whether accidental or deliberate) that could compromise security.

Compromise of information, loss of confidentiality, lack of integrity or unauthorised availability may result in harm to individual(s), reputational damage, detrimental effects on service, legislative non-compliance and/or financial costs and damages.

This Data Breach Reporting Policy (this Policy) outlines the institutional framework designed to ensure the security of all personal data at Multimatic during its life cycle, including the procedure to be followed to consistently and effectively manage data breach and information security incidents across Multimatic. This Policy supplements the Multimatic Data Protection Policy in relation to personal data protection breaches.

SCOPE

This Policy relates to all personal and sensitive data held by Multimatic regardless of format, and applies to all Multimatic employees, contractors, agency workers, consultants, interns, volunteers and other types of workers (together referred to as 'Employees' or 'you'). This Policy also applies to data processors working for, or on behalf of, Multimatic.

The objective of this Policy is to contain any personal data security breaches, to minimise the risk associated with any breach and consider what actions are necessary to secure personal data and prevent further breaches.

DEFINITION AND TYPES OF BREACH

For the purpose of this Policy, personal data security breaches include both confirmed and suspected incidents. An incident in the context of this Policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, which causes or has the potential to cause damage to Multimatic's information assets and/or reputation.

An incident includes, but is not restricted to, the following:

- loss or theft of personal data or special category data or equipment on which such data is stored (e.g. loss or theft of computer, laptop, USB stick, other electronic processing/storage device, or paper record)
- equipment failure
- unauthorised use of, access to, or modification of, data or information systems
- attempts (failed or successful) to gain unauthorised access to information or IT systems
- unauthorised disclosure of sensitive / confidential data, including personal data
- website defacement
- hacking attack
- unforeseen circumstances (such as a fire or flood)
- human error
- 'pretext' or 'blagging' offences - where information is obtained by deceiving the organisation which holds it

ADMINISTRATION OF POLICY

We do not have an appointed Data Protection Officer, and are not obligated to appoint one. For purposes of overseeing, advising on, and administering compliance with this Policy, the Data Protection Policy and the relevant data protection law/regulations, we will identify a Data Protection Lead within each division or facility, as appropriate. Usually, the Data Protection Lead will be a member of the HR department and will be the first point of contact on issues relating to data protection and any personal data breach.

REPORTING AN INCIDENT

Any individual who accesses, uses or manages Multimatic's information is responsible for reporting any personal data breach and information security incidents immediately or if the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable to HR-EU@Multimatic.com.

The personal data protection breach report will include:

- full and accurate details of the incident
- when the breach occurred (dates and times)
- who is reporting it
- the nature of the personal data information
- how many individuals are involved

All Employees should be aware that any breach of the Multimatic Data Protection Policy by an Employee may result in disciplinary action, up to and including the termination of employment or engagement.

CONTAINMENT AND RECOVERY

The Data Protection Lead will first determine if the breach is still occurring. If so, together with Multimatic IT, Corporate Security and other applicable resources (Response Team), the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the Response Team in liaison with relevant officers of the Multimatic to establish the severity of the breach and who will take the lead to investigate the breach (Lead Investigation Officer).

The Lead Investigation Officer, working with the Response Team and, if applicable, other subject matter experts, will establish whether there is anything that can be done to recover any losses and limit the damage of the breach. That group will also establish who may need to be notified as part of the initial containment and will inform Multimatic management and, where appropriate, the police.

The Lead Investigation Officer, in liaison with Multimatic management, will determine the suitable course of action to be taken to address and resolve the incident.

INVESTIGATION AND RISK ASSESSMENT

An investigation will be undertaken as soon as reasonably possible, but, generally, within 24 hours of the breach being discovered / reported.

The investigation will focus on the cause of the breach, the risks associated with it, and will take into account:

- the type of personal data involved
- its sensitivity
- the protections in place (e.g. encryptions)
- what happened to the data, whether it has been lost or stolen
- whether the data can be put to any illegal or inappropriate use
- the affected individuals, and the potential adverse consequences to them (including how serious/substantial these consequences could be, and the likelihood of occurrence)
- whether there are wider consequences to the breach

- other relevant considerations

NOTIFICATION

The Lead Investigation Officer, together with the Response Team, will determine who needs to be notified of the breach.

Every incident will be assessed in regards to notification on a case-by case-basis, including consideration of the following:

- are there any legal/contractual notification requirements
- will notification assist the individuals affected – can they take actions in relation to the information to mitigate risks
- will notification help prevent the unauthorised or unlawful use of personal data
- will notification help Multimatic meet its obligations under data protection law
- if a large number of individuals are affected or the consequences are very serious, does a supervisory authority under the GDPR or the Information Commissioner's office under the UK GDPR need to be notified.
- not every incident warrants notification and "over-notification" may cause disproportionate inquiries and unintended consequences.

If Multimatic discovers a personal data security breach that poses a risk to the rights and freedoms of individuals, we will report it to the relevant GDPR or UK GDPR supervisory authority within 72 hours of discovery. For details of the relevant supervisory/regulatory authority please refer to our Data Protection Policy.

If the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. To the extent feasible, specific and clear advice will be given on what they can do to protect themselves, including what actions have already been taken to mitigate the risks. Individuals will also be provided with contact details to allow them to contact Multimatic for further information or to ask questions on what has occurred.

The Lead Investigation Officer and Response Team must also consider notifying third parties such as the police, insurers, banks or credit card companies, etc. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The Lead Investigation Officer and Response Team will also consider whether it is appropriate to issue communications to other interested parties.

All actions will be recorded by the Lead Investigation Officer.

EVALUATION AND RESPONSE

Once the initial incident is contained, the Lead Investigation Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies or procedures are required.

Existing controls will be reviewed to determine their adequacy, and whether any corrective actions should be taken to minimise the risks of similar incidents occurring.

The review will consider:

- where and how personal data is held, stored and secured
- where the biggest risks lie, including any further potential weak points within the existing systems / data protection framework
- whether methods of transmission are secure, and compliant with the principle of data minimisation (only sharing the minimum amount of data necessary)
- identifying weak points within existing security measures
- staff awareness and training

- implementing a personal data breach plan and identifying individuals / functions responsible for reacting to reported breaches of security

Any report recommending changes to systems, policies and procedures relating to personal data protection will be considered and approved, as appropriate, by Multimatic's management.