Incident Handling and Data Breach Policy

Statement

Personal Audit Systems Ltd (hereinafter referred to as the "Company") are committed to our obligations under the regulatory system and in accordance with the GDPR to maintain a robust and structured program for compliance adherence and monitoring. We carry out risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognise that breaches can occur, so this document outlines our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from risks associated with processing data. The protection and security of the personal data is of paramount importance to us and we have developed specific controls and protocols for any breaches relating to the GDPR and data protection laws.

Purpose and Scope

The purpose of this document is to provide details of the Company's intent, objectives and procedures regarding data breaches involving personal information. Together with our obligations under the GDPR, we also have a requirement to ensure that correct procedures, controls and measures are in place.

This applies to all persons within the Company (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors.

We disseminate this to all employees ensuring they are aware of what the protocols and reporting requirements are for personal information breaches. Adherence is mandatory and non-compliance could lead to disciplinary action.

Data Security and Breach Requirements

The Company's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

We carry out information audits to ensure that all personal data processed by us is accounted for and recorded, alongside risk assessments that assess the scope and impact of any potential data breach; both on the processing and on a data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including (but not limited to):

- Encryption of personal data
- Restricted access
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services

- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and security testing on a regularly basis to test, assess, review and evaluate the effectiveness of all measures and compliance with the data protection regulations and codes of conduct
- Frequent and rolling training programs for all staff in the GDPR, its principles and applying those regulations to each role, duty and the company as a whole
- Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information
- Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorised by the Data Protection Officer

Objectives

- To adhere to the GDPR and EU Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and reducing the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes.
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect clients and staff – including their data, information and identity
- To ensure that the staff responsible is notified of the data breach (where applicable) with immediate effect and at the latest, within 72 hours after having become aware of the breach