DATA BREACH POLICY

General Data Protection Regulations (GDPR)

Introduction

RE Resource Group holds large amounts of personal and special category data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

This policy should be read in conjunction with the **Data Breach Procedure** document.

Scope

This policy relates to all personal and special category data held by RE Resource Group, regardless of format.

The policy applies to all staff, including temporary, consultants, suppliers and data processors working for, or on behalf of the Company. Any breach under GDPR may result in Disciplinary Procedures being instigated.

Purpose

Article 33 of the General Data Protection Regulations (GDPR) – Notification of a personal data breach to the supervisory authority – states that:-

"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."

Type of Breach

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

An incident is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

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

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g., loss of laptop, mobile phone, paper record).
- Equipment theft or 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 personal data or special category data.
- Website defacement.
- Hacking attack.
- Unforseen circumstances such as fire or flood.
- Human error.
- Offences where information is obtained by deceiving the organisation who holds it.

.

Reporting an incident

Any individual who discovers a data breach should report it immediately to the Data Protection Officer or the Central Support Team.

Further Information

If you have an questions regarding this Policy, please contact:-

James Gibbs
Data Protection Officer
RE Resource Group
7-9 Ambrose Street
Cheltenham
Glos
GL50 3QR

Tel. 01242 505400
jamesg@reresourcegroup.co.uk

or

Central Support Team (support@reresourcegroup.co.uk)