Data Breaches Policy

Under GDPR from 25th May 2018, there is a **breach notification duty** across the board.

Timing

QuiqSolutions are required to notify the **ICO (Information Commissioners Office)** within **72 hours** of any relevant data security breach. Fines may occur for any that are not notified within the timescales.

Relevant breaches are those where the individual is likely to suffer some form of damage, such as i**dentity theft** or a **confidentiality breach**.

Internal Reporting Policy

All members of the firm must be aware at all times of any instances that may occur which may give rise to a data protection breach.

Should you be aware of such a breach, this must be notified to your Line Manager immediately who in turn will notify the nominated Data Protection Manager within QuiqSolutions. This must be done immediately.

The Data Protection Manager will record all breaches within the **Data Security Incident Report** and notify the ICO if deemed appropiate.

When a **personal data breach** has occurred, you must establish the likelihood and severity of the resulting risk to the individual's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, therefore the reasons will be **documented and attached to the register.**

Reporting Policy to the ICO

If you need to report a breach.

- Go to ICO.gov.uk
- Select "Report a Breach"

There are 2 options for your firm to choose from:

1. **Report a Data Security Breach** – then follow the instructions
2. **Section 55 breach** – unlawful use of personal data

Complete the relevant section.

The ICO will report back to QuiqSolutions should any further information / action be required.

Reporting Policy to other persons / organisations

QuiqSolutions must inform the individual concerned regarding the data breach and the action taken. This must be actioned **immediately.**

QuiqSolutions must also decide whether other persons / organisations need to be information of the breach. This may include the client company or any other third parties involved.

Action required after any data breach

All data breaches must be discussed at Senior Management level and action taken to prevent any recurrence.

These actions must be documented and monitored on an ongoing regular basis to ensure any such breaches are not duplicated.

If staff discipline is required, please refer to your HR processes.

If the ICO require any further action, ensure this is advised to all Senior Management, action taken and fully documented.

Monitoring & Training

QuiqSolutions must ensure that there are **monitoring processes** in place to identify and prevent any data breaches.

QuiqSolutions must ensure that all staff are adequately trained on data protection and how to identify and prevent data breaches within their own particular roles.

The above must be fully documented.