EC Computers Ltd - Data Breaches Policy

Breach

Relevant breaches are those where the individual is likely to suffer some form of damage, such as identity theft or a confidentiality breach, and where the data breach is likely to "result in a risk for the rights and freedoms of an individual/s".

Breaches are not necessarily facilitated by a third party cyberattack or the like, and so the complexity of a ''Breach' can vary in its intensity, or in fact may not be a Breach at all.

Therefore, any situation should be tested against the following statement

"the data breach is likely to result in a risk for the rights and freedoms of individuals", ..

..and against the six GDPR Legal Conditions, which are known as "Lawfulness of processing conditions"

- *(a) Consent of the data subject*
- *(b) Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract*
- *(c) Processing is necessary for compliance with a legal obligation*
- *(d) Processing is necessary to protect the vital interests of a data subject or another person*
- *(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or Principal Data Protection Contact*
- *(f) Necessary for the purposes of legitimate interest pursued by the controller or Principal Data Protection Contact or by a third party, except where such interests are overridden by the interests, rights or freedoms of a data subject*

Timing

EC Computers are required to notify the ICO (Information Commissioners Office) within 72 hours of any relevant data security 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 EC Computers. This must be done immediately.

The Data Protection Manager will record all breaches within the Data Security Incident Report and notify the ICO should the breach be identified as relevant to report.

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 – the process is as follows –

Go to ICO.gov.uk – for organisations -

On this page you will find on the right-hand side "Report a Breach"

Within this section, 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 EC Computers should any further information / action be required

Reporting Policy to other persons / organisations

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

EC Computers 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.

Test the 'Breach' situation against the content of the opening section – 'Breach'

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

EC Computers must ensure that there are monitoring processes in place to identify and prevent any data breaches

EC Computers 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