CRBDirect

BREACH REPORT POLICY AND PROCEDURE

Personal data and breaches and notification

Under the General Data Protection Regulation, ('GDPR'), all breaches will have to be reported. Although this obligation applies with the incurrence of a breach of any level of severity, particular attention must be paid by a firm to those breaches which are likely to result in a high risk to the rights and freedoms of individuals.

For the purpose of clarity, a 'high risk' means the threshold for notifying individuals is higher than for notifying the Information Commissioner's Office; a notification must be made directly and immediately. High risk may result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

In case of an incident defined as, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed", the new breach notification regime under the GDPR will apply as follows:

1. *Obligation for data processors to notify data controllers*

Timing:

Without undue delay after becoming aware of it.

Exemption:

None in the GDPR

Observations:

• All breaches will have to be reported.

• EDPB to issue guidelines to clarify the notion of “undue delay” and the particular circumstances in which a data processor is required to notify the personal data breach.

2. Obligation for data controllers to notify the supervisory authority

Timing:

Without undue delay and, where feasible, not later than 72 hours after becoming aware of it.

Exemption:

No reporting if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Observations:

• When the timing obligation is not met, reasons will have to be provided to the supervisory authority (e.g. request from a law enforcement authority).

• EDPB to issue guidelines to clarify the notion of “undue delay” and the particular circumstances in which a data controller is required to notify the personal data breach.

2. *Obligation for data controller to communicate a personal data breach to data subjects*

If the data controller is yet to do so, the supervisory authority may compel the data controller to communicate a personal data breach with affected data subjects unless one of the three exemptions is satisfied.

Timing:

Without undue delay: the need to mitigate an immediate risk of damage would call for a prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for communication.

Exemption:

No reporting is required if:

• The breach is unlikely to result in a high risk for the rights and freedoms of data subjects and this can be demonstrated. For example, the data may have been rendered unintelligible through encryption. Please see the regulatory risk assessment for more detail;

• Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or

• This would trigger disproportionate efforts (instead a public information campaign or “similar measures” should be relied on so that affected individuals can be effectively informed)

CRBDirect

Documentation requirements in relation to breach reporting

In respect to our duties under the General Data Protection Regulation, our firm will ensure that it maintains:

• An internal breach register: this is an obligation for the data controller (our firm) to document each breach incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken". The supervisory authority may be requested to assess how data controllers comply with their data breach notification obligations.

• There are also prescribed requirements to satisfy in the communication to the supervisory authority, e.g. o Describing the nature of the personal data breach, including, where possible, the categories and approximate number of data

subjects concerned, and the categories and approximate number of data records concerned, etc.

• The communication to affected individuals e.g. o Describe in clear and plain language the nature of the personal data breach and provide at least the following information:

(i) the name and contact details of the Data Protection Officer or other contact point where more information can be obtained; (ii) the likely consequences of the personal data breach; and (iii) the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects).

Failure to meet the above requirements exposes the organisation to an administrative fine of up to €10,000,000 or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In general, the GDPR establishes a tiered approach to penalties for breach which enables the DPA's to impose fines for some infringements of up to the higher of 4% of annual worldwide turnover and €20,000,000. Other specified infringements would attract a fine of up to the higher of 2% of annual

worldwide turnover and €10,000,000. A list of points to consider when imposing fines (such as the nature, gravity and duration of the infringement) is included.

These percentages apply to an 'undertaking' and a last-minute clarification in the Recitals adds that this is defined in Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU).

DATA SECURITY BREACH REGISTER

Elucidate Contractor Services (ECS) Limited must also keep own record of all personal data breaches in an inventory or log.

It must contain at minimum:

• the facts surrounding the breach;

• the effects of the breach; and

• remedial action taken

In the event of any data security breach, we will always aim to submit as much information as possible, for both the benefit of the Regulator and for our own benefit so as to mitigate the risk of any reoccurrence of the breach.

Wherever a data security breach occurs we will document all available information so that the information can be presented to the regulator within the required timeframe of 72 hours following the occurrence of that breach. We will also use this information to mitigate against the risk of any reoccurrence of the breach. That information will include:

• Firm's name

• Date of breach

• No people affected
• Nature of breach (choose most relevant)
• Description of breach
• How you became aware of breach
• Description of data
• Consequences of breach
• All individuals informed
• Remedial action
• Other Regulators informed
• When did you first notify the ICO of the breach?

Elucidate Contractor Services (ECS) Limited must also submit this log in a form format set (available on ICO's website) to ICO, on a monthly basis.

PERSONAL DATA BREACH REGISTER

A personal data breach may mean that someone other than the data controller (our firm) gets unauthorised access to personal data. But a personal data breach can also occur if there is unauthorised access within an organisation, or if a data controller's own employee accidentally alters or deletes personal data. In the event of a breach we will notify the Information Commission's Office ('ICO') within 24 hours of becoming aware of the essential facts of the breach. Our notification to the ICO will include as a minimum:

• Our name and contact details;
• The date and time of the breach (or an estimate);
• The date and time we detected it;

• Basic information about the type of breach; and

• Basic information about the personal data concerned.

We are aware that a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

RECORDS HANDLING AND RETENTION PROCEDURE

Senior Management needs to ensure that the records can be made available for regulator inspection. Where records are stored electronically, they need to be reproduced, unchanged from their original content, stored so that they cannot be accidentally deleted and are regularly backed-up. Staff must adhere to the policy that documents which contain sensitive data are destroyed appropriately.

The firm may be able to hold personal data for as long as they have consent to do so or until a purpose/service has been fulfilled. As described below, if the firm is required to hold certain types of personal information for specific purposes such as complaints, or for any other superseding law (such as employment) this information must be kept to a minimum or archived/encrypted to ensure no further processing of that information occurs.

CRBDirect

Records Retention

Accounts Records. - Three years from the end of the accounting period.
Financial Records. - In line with Inland Revenue requirements, we retain financial records including bank statements for 6 years.
Agency and Customer Agreements. - Six years from the date of termination.
Data Suppliers and Lead Generators details and agreements. - Three years from the termination of the contract of appointment.
Complaints. - Three years from the date of receipt.
Document reference numbers and print dates of third party documents provided to customer. - Three years from the date it was provided.
Reference copies of own documentation supplied to customers. - Three years from the date it was provided.
Management Structure - Six years from the date of any change.

Training Records. - Three years from the date employment ceased.

All records, particularly confidential records, will be securely retained. Measures could include:

- Keeping all paper records locked in secure cabinets at the end of the business day.
- Encrypting all digital records.
- Confidential e-mails including customer details to be sent by secure methods and encrypted.
- Maintaining a ‘clear-desk’ policy.
- Company computers to be password-protected.

CRBDirect

• Confidential records to be stored on drives with limited access to authorised staff only.

MONITORING

On a regular basis, management will confirm that we maintain appropriate protection of data. Periodically, checks will be made confirming data is retained securely, that cabinets are locked, and computers are 'shut-down' (or secured) after close of the business day.

We will maintain a 'clear-desk' policy and ensure that correct encryption procedures are followed.

We will maintain a record of all subject access requests and ensure we follow all appropriate data protection regulations.

Only authorised staff will be allowed access to data and we will maintain records of access authorities.

On an annual basis, we will conduct an audit of retained data to ascertain whether any is due for destruction.