# BREACH REPORT POLICY AND PROCEDURE

**Personal data and breaches and notification**

Under the General Data Protection Regulation, ('GDPR') certain breaches which include personal data will have to be reported.

Breaches which include personal data are reportable to the supervisory authority the Information Commissioner's Office (ICO), unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals concerned.

Breaches which include personal data and are likely to result in a high risk to the rights and freedoms of the individuals need to be notified to those affected.

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

**Timing:**
Without undue delay after becoming aware of it.

**Exemption:**
None

**Observations:**

- All breaches to be reported to the data controller by the data processor.

*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

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

**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 communication is required:

• Unless the personal data breach is likely to result in a risk to the rights and freedoms of the data subject

IN THE EVENT OF A BREACH OR SUSPECTED BREACH WHICH INCLUDES PERSONAL INFORMATION, THE CONTROLLER AND OR PROCESSOR MUST IMMEDIATELY TAKE ACTION TO STOP THE BREACH CONTINUING OR RECURRING.

**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. 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. 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.

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 if required 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?

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 being reportable we will notify the ICO within 72 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

Whether a personal data breach is considered reportable, or not, it will be recorded in the Personal Data Breach Register.

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.

Refer to our DATA BREACH LOG