Data Breach Notification Policy (GDPR compliant)

Aim and scope of policy

The Company is fully aware of its obligations under the General Data Protection Regulation (GDPR) to process data lawfully and to ensure it is kept securely. We take these obligations extremely seriously and have protocols in place to ensure that, to the best of our efforts, data is not susceptible to loss or other misuse.

The GDPR incorporates a requirement for a personal data breach to be notified to the supervisory authority and in some cases to the affected individuals. This policy sets out the Company's stance on taking action in line with GDPR if a breach were to occur.

Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed. A 'breach', for these purposes, is identifiable as a security incident which has affected the confidentiality, integrity or availability of personal data.

As indicated above, a data breach for these purposes is wider in scope than the loss of data. The following are examples of data breaches:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a data controller or data processer
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

Breach detection measures

The systems are protected by various layers of security to prevent unauthorised access. Where settings and features within applications are available these will be used to assist staff in sense checking what they are sending (Outlook DLP).

The Company may also become aware of a personal data breach from a member of staff, a client/customer, a member of the public etc. Charles Wells staff are aware of what constitutes a breach, so they can notify the internal Compliance Team as soon as they become aware that one may have occurred.

Notifiable breaches

For the purposes of this policy, a data breach will be notifiable when it is deemed by the Company as likely to pose a risk to people's rights and freedoms. If it does not carry that risk, the breach is not subject to notification although it will be entered on the Company's breach record.

A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

When assessing the likelihood of the risk to people's rights and freedoms, the Company will consider:

- the type of breach
- the type of data involved including what it reveals about individuals
- how much data is involved
- the individuals involved e.g. how many are involved, how easy it is to identify them, whether they are children etc
- how bad the consequences for the individuals would be and
- the nature of the Company's work and the resultant severity of a breach.

Actions upon identification of breach

When the Company is made aware of a breach, it will undertake an immediate investigation into what happened and what actions must be taken to restrict any consequences. A determination will be made at that point whether the breach is deemed a notifiable breach and whether it is deemed as resulting in a high risk to the rights and freedoms of individuals.

Timescales for notification to supervisory authority

Where a notifiable breach has occurred, the Company will notify the Independent Commissioner's Office (ICO) without undue delay and at the latest within 72 hours of it becoming aware of the breach. If notification is made beyond this timeline, the Company will provide the ICO with reasons for this.

If it has not been possible to conduct a full investigation into the breach to give full details to the ICO within 72 hours, an initial notification of the breach will be made within 72 hours, giving as much detail as possible, together with reasons for incomplete notification and an estimated timescale for full notification. The initial notification will be followed up by further communication to the ICO to submit the remaining information.

Content of breach notification to the supervisory authority

The following information will be provided when a breach is notified:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned and
    - the categories and approximate number of personal data records concerned
- the name and contact details of the CW Compliance Team where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Timescales for notification to affected individuals

Where a notifiable breach has occurred, which is deemed to have a high risk to the rights and freedoms of individuals, the Company will notify the affected individuals themselves i.e. the individuals whose data is involved in the breach, in addition to the supervisory authority. This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

Content of breach notification to the affected individuals

The following information will be provided when a breach is notified to the affected individuals:

- a description of the nature of the breach
- the name and contact details of the CW Compliance Team where more information can be obtained
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Record of breaches

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach and its effects.