Wells & Co Data Breach Notification Policy (UK GDPR compliant)

WELLS & Co
EST ▲ 1876

Aim and scope of policy

The Company is fully aware of its obligations under the UK General Data Protection Regulation (UK 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 UK 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 expectations in line with UK GDPR, of anyone who works for the Company and discovers or suspects that a breach has occurred.

Personal data breach

A personal data breach has two elements. Firstly, there must be a breach of security, which for these purposes means a security incident which has affected the confidentiality, integrity or availability of personal data. Secondly, that breach of security must have led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data which was being transmitted, stored or processed by us. It doesn't matter if the breach was accidental or deliberate, nor if it was done by someone inside or outside the Company.

As indicated above, a data breach for these purposes can cover a lot more than just 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.

Why this is so important

Identifying and reporting data breaches is a really important part of keeping the Company safe. Knowing about a breach promptly gives us a chance to correct altered information, retrieve something that has gone astray, and close of unauthorised access. This helps the Company work more efficiently, but it also limits the risk of enforcement action (including fines and negative publicity) from regulators, and reduces the chance of the Company being sued by individuals whose data has been caught up in the breach. Those risks are real, which is also why we have a clear notification policy that **must** be followed whenever you think there has been a breach.

Breach detection measures

The Company's 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 provided with guidance and training to tell them what a breach looks like. Anyone can make a mistake, and there will always be those outside the Company looking to gain access to our systems for their own purposes. We all have a role to play in being on the look-out for something that has gone wrong, and letting the CW Compliance Team know as soon as possible if we think that a breach has occurred.

Notifiable breaches

All breaches (even suspected breaches) must be reported to the CW Compliance Team. They will decide whether a breach is "notifiable", or in other words whether it needs to be reported to anyone outside of the Company.

For the purposes of this policy, a data breach will be notifiable when the Company thinks that it is 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 and might need to be reported to some of the other companies that we work with.

A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss, emotional distress, 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 (e.g. whether it was an accident, or a deliberate hack)
- the type of data involved including what it reveals about individuals
- how much data is involved
- the individuals who might be affected (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
- how severe the breach is, having regard to the nature of the Company's work.

Actions upon identification of breach

When the Company is made aware of a suspected or actual breach, it will undertake an immediate investigation into what happened and what actions must be taken to restrict any consequences. A decision will be taken at that point about whether the breach is notifiable and whether it is likely to result 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 Information Commissioner's Office (ICO) without undue delay and at the latest within 72 hours of the Company 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.

Care must be taken with these notifications, which could affect the decision which the ICO makes, but which also could be used as evidence in legal proceedings involving the Company. This is why all notifications are handled by the CW Compliance Team, with legal advice as necessary.

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, and the breach is one which is likely to present a high risk to the rights and freedoms of affected individuals, the Company will also have to notify the affected individuals themselves.. This notification will be made without undue delay and may, if the risk to the affected individuals is immediate, need to 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.

As with the notifications to the ICO, great care must be taken with the contents of these notifications which are public documents and may be supplied to the media, to competitors, to the regulator, or to lawyers looking for evidence to enable them to make claims against the Company. Even if you think it is very important that an individual should be told about a breach straightaway, please make sure to involve the CW Compliance Team in that decision, and do not send any notification to anyone without their approval.

Record of breaches

The Company records all personal data breaches and "near misses" regardless of whether they are notifiable or not. This is part of the Company's general accountability requirement under UK GDPR. It records the facts relating to the breach and its effects. This helps us to identify patterns of risk and areas to focus on for training or additional protections, and will enable the regulator to understand how we have monitored and assessed the risks faced by the business.

Thank you for your assistance in this important work of keeping the Company safe.