DATA BREACH PROCEDURE

What is Data Breach?

A Personal Data Breach can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- 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

A breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

Procedure to Report a Data Breach

As soon as it has become apparent, or suspected, that a personal data breach has occurred, the Company's GDPR Compliance Manager should be notified as soon as possible via gdpr@bytes.co.uk providing as much detail as possible.

On becoming aware of a breach, the Compliance Manager will work with the relevant departmental managers to assess the severity of the data breach and inform the Board. Bytes will try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

Reporting the Data Breach to the ICO

When a personal data breach has occurred, the likelihood and severity of the resulting risk to people's rights and freedoms will be established. If it is likely that there will be a risk then the ICO will be notified; if it is unlikely then the ICO need not be informed. Where we decide not to report the breach, it will be documented to justify this decision.

Where Bytes uses a data processor, and the processor suffers a breach, they must inform us without undue delay as soon as they become aware; Bytes will then notify the ICO of the data breach.

ICO: www.ico.org.uk

ICO Reporting Timescales

A notifiable breach will be reported to the ICO without undue delay, but no later than 72 hours after becoming aware of the breach. If it takes longer, then reasons for the delay will be given.

As it is not always possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it, the required information can be provided in phases, as long as it is done without undue further delay.

Information required for the ICO

When reporting a breach to the ICO it will include:

- 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 data protection officer (if your organisation has one) or other contact point 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.

Notifying the Individual of a Data Breach

The individual will be notified of a breach where it is likely to result in a high risk to the rights and freedoms of the individual.

- When notifying the individual of a data breach, it will be done using clear and plain language and describing the nature of the personal data breach and, at least include:
- the name and contact details of 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 and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

Recording of Data Breaches

Regardless of whether or not a data breach was reported to the ICO, all breaches will be recorded. It will record the facts relating to the breach, its effects and the remedial action taken.

Remedial Action of Data Breaches

All breaches will be investigated to establish whether or not it was a result of human error or a systemic issue and see how a recurrence can be prevented; whether that be through better processes, further training or other corrective steps.

Relating Documents

Please also read the Company's Information Security Incident Management Policy.