Data Breach Policy

Introduction

Burlington Uniforms acknowledges that the UK General Data Protection Regulation imposes on it an obligation to report certain types of personal data breach to the Information Commissioner. This must happen within 72 hours of becoming aware of the breach, where feasible.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must be informed without delay.
- The company seeks to ensure that it has robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not the company is required to notify the relevant supervisory authority and the affected individuals.
- The company will keep a record of any personal data breaches, regardless of whether it required to notify.

Data Protection Team

The Data Protection Team will be responsible for the formulation, implementation and review of this policy. The Team will be constituted by:

Adrian Hewitt (Managing Director and Confidentiality Officer)
Tristan Weedon (General Manager)
Peter Blunden (Systems and Quality Manager)

Definitions

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Notifiable Breach (Information Commissioner) means a breach following which it is likely that there is a risk to individuals' rights and freedoms.

Notifiable Breach (Individual) is a breach which is likely to result in a high risk to the rights and freedoms of individuals.

Rights and freedoms of individuals includes the freedom of association, employment, movement, person, speech, work or professional practice or any other activity not restricted by lawful authority; right to integrity of the person including mental and emotional well-being; rights in or over real or personal property including information and intellectual property; rights to confidentiality, privacy, reputation and standing and right not to suffer discrimination.

Data Breach Policy

Assessment of Risk

Every risk identified is assessed and scored for both Impact and Likelihood on a Low/Medium/High scale. The following definitions and scoring criteria used:
Impact is the measure for any particular uncertainty of the effect on the rights and freedoms of individuals.

Low	Effect would be insignificant or manageable with available resources.
Medium	Would cause difficulties requiring significant or diversion of (or new) resources by individuals affected by the breach.
High	Effect would be serious enough seriously to undermine, cause loss, damage or put to expense the individuals whose data has been affected by a data breach and could require intervention or assistance by third parties to mitigate loss or prevent further loss or damage.

Likelihood is the expected probability of the occurrence of the uncertain event assessed after taking into account any mitigating factors and the active management or operational actions in place to reduce the likelihood.

Low	Extremely unlikely
Medium	Possible but not very likely
High	Probable

The risk order is generated with reference to the combination of the two scores as First, Second or Third Order according to the risk order matrix set out in Appendix 1 of POL 013 (Risk).

Occurrence of Breach

Any employee who discovers a data breach or has a data breach reported to him or her will immediately inform the Confidentiality Officer or other member of The Data Protection Team.

The Data Protection Team will immediately try to assess what is the cause and nature of the breach, whether it is deliberate or accidental, immediate corrective action, corrective action to prevent recurrence and whether the breach is reportable. If the Team is unable to assess all or any of these factors it will immediately call in the Company's IT support company, Replentec, who provide 365 days a year cover and have remote access to the company's IT system.

The Data Protection Team will record: a summary of the event and the circumstances (time, date, who discovered/reported, incident, responsibility), the data impacted, the individuals or group(s) of individuals affected, the risk of harm, the likely consequences of the breach, corrective and preventive action and the likelihood of recurrence.

If the Data Protection Team considers that the risk is not reportable it will record the reasons for so deciding. If in doubt the Team will report. If it is reportable it will complete FOR 085. Copies will be sent to the Information Commissioner and (if required) to the individuals affected or likely to be affected. The Confidentiality Officer will keep an office copy of the completed form.

Reports must be transmitted within 72 hours. If this is not possible the reason must be provided to the Information Commissioner and the individuals to whom reports are being sent.

Related Documents

Burlington Uniforms maintains a Policy on Security and Confidentiality (POL 007). Amongst other matters this sets out basic protocols to be followed on a day-to-day basis to prevent accidental loss or deliberate misuse of data. It also sets out the System Security Measures that are in place to prevent the leaking of data to unauthorised sources and the protection of our systems from cyber attacks.

General Matters

This policy is a document within our Integrated Management System. It will be reviewed annually and following review circulated to all staff to be read and signed as read.

Signed: 

Adrian Hewitt
Managing Director

Date: 21st July 2023
Review Date: 19th July 2024