Bell Apparel Ltd

Data Privacy and Protection Policy

Introduction

Bell Apparel is fully committed to compliance with the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), effective from the 25 May 2018, and the Data Protection Act 2018. The company will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants, partners or other servants (all now referred to as 'staff') of the company who have access to any personal data held by or on behalf of the company, are fully aware of and abide by their duties and responsibilities under the GDPR.

Statement of policy

In order to operate, Bell Apparel has to collect and use information about people with whom it works. The data collected for each type of person is as follows:

Customers (wearers) – we collect data required to identify the individual and their employer. We also collect sizing data to ensure that the PPE we supply meets their requirements.

Bell Apparel staff – we collect personal data in order to form a legal employee to employer relationship. We also collect data to make sure we can pay our staff and provide benefits to them.

Clients and suppliers – we collect personal data in order to communicate to these people about the service. This is 'business card' data.

In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

Personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the GDPR to ensure this. Bell Apparel regard the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the company and those with whom it carries out business. The company will ensure that it treats personal information lawfully and correctly.

The principles of data protection

The GDPR has principles which should underpin the way personal data is processed. Bell Apparel fully endorses and adheres to these principles. Personal Data:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be kept secure i.e. protected by an appropriate degree of security;

Handling of personal/sensitive information

Bell Apparel will, through appropriate management and the use of strict criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information, informing the Data Subjects as appropriate;
- Ensure that data it holds is processed legally;
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used;
- Keep data only for a pre-determined length of time and only for as long as is required;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that the rights of people about whom the information is held can be fully exercised under the GDPR.

In addition, Bell Apparel will ensure that:

- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately and regularly trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- New starters will be similarly trained at induction;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.
- Personal data that originated within the EU will not be shared with any companies or individuals outside the EU.

All managers and staff within the company will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All staff of the company must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the company, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the GDPR. Any breach of any provision of the GDPR will be deemed as being a breach of any contract between the company and that individual, company, partner or firm;

All contractors who are users of personal information supplied by the company will be required to confirm in writing that they will abide by the requirements of the GDPR with regard to information supplied by the company.

Authority

The company has appointed an Information Security Officer. This officer will be responsible for ensuring that the Policy is implemented. This officer will have overall responsibility for:

- The provision of cascade data protection training, for staff within the company.
- For the development of best practice guidelines.
- For carrying out checks to ensure continual adherence to the GDPR.

The Information Security Officer should be contacted as soon as possible if:

- There is a complaint against any reported data inaccuracy;
- There is an actual or suspected data breach (see below);
- Bell Apparel receives a Subject Access Request;

Data Breach

Bell Apparel has a Data Breach process in place. All staff should make sure they understand their requirements under this process and, in the event of an actual or suspected data breach, should follow the process and notify the Compliance Officer immediately.

Subject Access Requests

Bell Apparel has a Subject Access Request process in place. All staff should make sure they understand their requirements under this process and, in the event of a subject access request, should follow the process and notify the Compliance Officer as soon as practical.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data processors. Bell Apparel is registered as such. This regulation requires every company that is processing personal data, to notify and renew their notification, on an annual basis.

I P Mitchell
Managing Director

Date of Issue: 14 May 2020