Data Protection Policy

Applicable to – All departments of the Bellsure Group, i.e. Streetsure, Vista, and Styletech (Referred to as 'Bellsure').

Purpose of policy – To ensure all personal information obtained, used, and shared by Bellsure in its work is treated with appropriate care and respect, and is used lawfully and fairly in conjunction with GDPR

Introduction

Personal data is regulated by the General Data Protection Regulation and is defined as '*any information relating to an identifiable natural person (A living human being)*'

Everyone who works for Bellsure uses personal information.

Scope

This document applies to all employees, subcontractors, and agents of Bellsure who process, have access to, or have custody of Bellsure information.

All employees must understand and adhere to this policy and are responsible for ensuring the safety of all information processed by Bellsure. All employees have a role to play and a contribution to make to the safe and secure use of information they hold.

Principles

The GDPR is based on seven principles relating to the lawful processing of personal information. Compliance with these principles ensures information is secure, well-managed, accurate, and available. Personal information can be obtained, used, shared, and kept for providing services to our customers and employees, looking after people's interests, and supporting Bellsure's legitimate interests.

1. Personal data shall be processed lawfully, fairly, and transparently
2. Personal data shall be collected for specified, explicit, and legitimate purposes
3. The Personal Data collected and processed shall be adequate, relevant, and limited to what is necessary
4. Personal Data shall be accurate and, where necessary, kept up to date
5. Personal Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it was originally collected
6. Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful access and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
7. The Appointed Data Person within Bellsure shall be responsible for and able to demonstrate compliance with all of the above principles.

Rights

The GDPR rights of the data subject are explained here – https://ico.org.uk/for-the-public/is-my-information-being-handled-correctly/

Employees' Responsibilities

Bellsure holds information about customers and prospective customers, employees, job applicants, subcontractors, and suppliers. Everyone who works for or represents Bellsure must protect the personal information that they use and be aware of their obligations.

Employees cannot use personal information obtained at work for their own purposes. Employees who knowingly disclose or misuse Bellsure information for their own purposes, or who knowingly ignore the requirements of this policy will face disciplinary action, regardless of any possible criminal sanctions. This could lead to summary dismissal for gross misconduct and breach of trust. This also applies to former employees of Bellsure.

Awareness and Training

Bellsure promotes the need to respect privacy and confidentiality so that customers remain confident about trading with Bellsure. People must be told how Bellsure will use their information, so that they are not reluctant to provide it to us.

Appropriate confidentiality and data protection training must be completed by all employees once a year, and prior to them having access to any personal information.

Collecting Information

People must be informed when Bellsure record information about them. Any process involving the collection and use of personal information must conform to the principles of the GDPR.

Bellsure will collect personal information from people only in the following circumstances –

- Where we have their freely given and informed consent
- Where we need the information to perform a contract involving them, or where we need the information to prepare to enter into a contract involving them
- Or where it is in our legitimate interests and is not overridden by their data protection rights

In some cases, Bellsure may have a legal obligation to collect personal information or may need the personal information to protect the data subject's vital interest or those of another person.

If we ask someone to provide personal information we will make it clear at the time and advise them whether the provision of their personal information is mandatory or not, and we will also advise them of the possible consequences if they do not provide their personal information.

(Bellsure Data Protection Policy p.2)

Similarly, if we rely on our legitimate interests (or those of any third party) when we collect and use someone's personal information, we will make it clear at the time what are those legitimate interests.

Customers

Bellsure holds the details of the organisations that have requested our services in order to provide those services (Including contract details of people working for those organisations). However, we only use these details to provide the service that the organisation has requested and for other closely related purposes.

Personal information we collect will be retained where we have an ongoing legitimate business need to do so (e.g. to provide a service or to comply with applicable legal, tax, or accounting requirements).

E mail addresses of customer contacts may be used for targeted advertising campaigns, which can include direct e mails and targeted advertisements through social media platforms.

Prospective Customers

Where promoting our services we may purchase databases of business contacts within our target sectors. These contacts will only be purchased from credible sources who can provide sufficient assurances that they are meeting their data protection obligations. These providers include such as Barbour ABI contract research.

Employees and Job Applicants

Bellsure only uses the information provided during the application process to progress the job application, or to fulfil legal or regulatory requirements. Bellsure will use the applicant's contact details to contact the applicant and progress the application. Bellsure will use the information provided by the applicant to assess the applicant's suitability for employment at Bellsure.

Bellsure will collect and use the personal information of employees to fulfil their contract of employment or to protect the vital interests of the employee or some other person.

Bellsure does not share any of the provided information with any third parties for marketing purposes. Data sent electronically or processed beyond the initial application will be stored within the European Economic Area. The information provided will be held securely by Bellsure and/or their data processors whether the information is in digital or some physical format.

Subcontractors and Suppliers

Bellsure will collect and use the personal information of subcontractors and suppliers in order to fulfil any contract in which they are involved.

Protection and Privacy by Design and Default

When developing new services or processes Bellsure needs to understand the legal basis for processing personal information and will carry out a Privacy Impact Assessment (PIA) when designing all new initiatives or changes to existing services or processes.

The PIA will identify any privacy or data protection concerns and ensure they are addressed before the project is implemented. If consent is needed to use personal information, it will be obtained as soon as possible. If consent is not required, we will still tell people how their information will be used.

Forms and Tools for Gathering Information

Any form or process designed to gather personal information must include a simple explanation about why the information is needed, and how it will be used and if shared with any third parties.

Records Management

Bellsure will maintain records management, retention and disposal procedures, including measures to ensure that personal information and working records are accurate, up to date, relevant, adequate but not excessive. Bellsure will ensure that it is easy for employees and customers to update their personal information, where appropriate. Inaccuracies will be corrected as soon as they come to light.

Records must be disposed of securely in accordance with the appropriate disposal schedule found within the Records Management Policy. Records management procedures, including retention and disposal, apply equally to paper and electronic records including e mails.

Bellsure will retain all employee information for seven (7) years beyond the date that an employee last worked for the Company. Beyond that time, Bellsure will destroy all information about that particular employee other than that information which Bellsure may be required to retain by law, and information that would allow Bellsure to furnish a reference for that employee in the future.

For full information on our records management please refer to the Records Management Policy.

Need to Know

Employees must not disclose confidential information to anyone who does not need it, unless the information is about serious wrong-doing or harm. All employees have a duty to report any criminal activity or wrongdoing to the proper authorities. Information must only be passed beyond Bellsure employees with the written consent of a Bellsure Director.

Physical Security

The Appointed Data Person must be notified of any loss, theft, or accidental disclosure of personal information.

Access to locations where information is held must be controlled, paper files containing personal information must be locked away when not in use, and computer data must be protected adequately.

(Bellsure Data Protection Policy page 3)

Access to information must be restricted to authorised employees only; such employees must receive training on the security of the system prior to being given access to any personal information. If at any time personal information is stored on a laptop or smartphone, it is the responsibility of the user to ensure that the information is secure and is regularly backed up.

Employees must not give unauthorised users access to devices on which other clients' records are displayed or could be accessed.

Care must always be taken if personal information is used outside the office, whether it is on paper or in a computer file. Personal information must only be stored on devices or equipment which are appropriately protected against viruses, malware, etc. Encrypted files should be used where dangers exist.

Bellsure protects its approved systems using WATCHGUARD firewalls. E mails are further scanned using MIMECAST. The main server is protected and managed by our third-party IT contractors, Neuways.

Contracts

All contracts should include clauses to ensure that Bellsure's data is used safely and appropriately. Information supplied to third parties must only be used for agreed purposes.

Due diligence must be carried out in relation to all contracts of agreements that involve the sharing of personal information. Risk assessments are required to assess the organisational maturity of a third party's data protection processes. All contractors that need access to Bellsure's information will be required to undertake regular data protection training.

Subject Access Requests (SAR's)

Employees and Bellsure workers (e.g. Subcontractors) will assist individuals who wish to gain access to the personal information we hold about them by referring them to the Appointed Data Person.

All SAR's must be answered within 20 working days. When someone requests information we hold, we will –

- Give them a description of the information;
- Let them know why we are holding it;
- Let them know who it may be shared with (if anyone); and
- Give them a copy of the information in a structured, commonly used digital format.

Bellsure must ask that the individuals requesting personal information we hold will put their request in writing to the Appointed Data Person whose details are given below.

Complaints

Bellsure takes any complaints very seriously. If someone believes that our collection or use of information is unfair, misleading, inappropriate or inaccurate, we encourage them to bring it to our attention so that we can deal with the complaint.

If a person identifies inaccuracies in the personal information, we hold about them, those inaccuracies must be corrected immediately.

If a person objects about unfair use of their personal information, the Appointed Data Person should investigate the complaint and will either suspend the processing of that person's data or explain to the person why Bellsure need to continue processing their information.

Contact Details for Appointed Data Person

The address of the Appointed Data Person is as follows –

The Appointed Data Person, Bellsure Supplies Ltd, Vision House, Bedford Road, PETERSFIELD, GU32 3QB

Or by e mail to info@bellsure.co.uk

Email

Bellsure encrypts and protects e mail traffic. If your e mail service does not support this, you should be aware that any e mails we send or receive may not be protected in transit.

Bellsure also monitors all e mails, including file attachments, for viruses or malicious software, and has Mimecast system to guard against the majority of rogue e mails

Contacting Bellsure Through the Website

If someone signs up Bellsure information or newsletter or fills in the contact form on the Bellsure website contact page, Bellsure will receive an e mail which contains their name, e mail address, company name, and the contents within any additional field. This information will not be shared with any other organisation.