SERTUS™

Data Protection Policy

Policy last approved: 01.08.23 **Next review date:** 01.08.24

Introduction

Sertus Limited (referred to as Sertus in this Policy Document) needs to gather and use certain information in relation to business activities. This information can include details about customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy sets out the standards which Sertus must comply with when collecting, handling, disclosing or otherwise using information about individuals (personal data). These standards are required by law and substantial fines and other sanctions may result from non-compliance. It is also a matter of good business that we treat information and data with appropriate care.

Compliance with this policy is mandatory. Failure to comply may lead to disciplinary action being taken that could ultimately result in termination of employment.

Scope

This policy applies to all employees, volunteers and temporary staff. It is our responsibility to ensure all of our suppliers and other third parties who store, access or otherwise use personal data on our behalf also comply with the requirements of relevant GDPR in force from time to time.

This policy is supplemented by additional guidance for those areas of each business that regularly deal with personal data:

1. HR
2. Payroll
3. Pensions
4. IS/ICT
5. Sales, Marketing, and Customer Relations
6. CCTV

It is mandatory for employees that work in the areas identified above to read and comply with the guidance that relates to their area.

This policy helps to protect Sertus from data security risks, including:

- Breaches of confidentiality (for example, information being given out inappropriately)
- Failing to offer choice (for example, all individuals should be free to choose how the company uses data in relation to them)
- Reputational damage (for example, the company could suffer if unauthorised users successfully gained access to sensitive data)

These identified people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that Sertus meets its legal obligations.

The Data Protection Officer is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues

- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy
- Handling data protection questions from staff and anyone else covered by this policy
- Dealing with requests from individuals to see the data Sertus Ltd holds about them (also called 'subject access requests')
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

The IT Manager is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services the company is considering using to store or process data (for instance, cloud computing services)

The Marketing Manager is responsible for:

- Approving any data protection statements attached to communications such as emails and letters
- Addressing any data protection queries from journalists or media outlets like newspapers
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principals

Personal Data

The law applies to "personal data". This is information about a living person. It includes both information about them (e.g. name, age, e-mail, address, job title, sex) as well as opinions about them. We typically hold personal data about potential, current and former employees, customers and suppliers.

Special precautions must be taken when dealing with sensitive personal data. "Sensitive personal data" includes information about someone's physical or mental health (including that someone is in good health), political or religious beliefs, racial or ethnic origin, trade union membership, and sexual orientation as well as genetic and biometric information. The circumstances in which this data can be collected and used are limited and no one should have access to, or deal with, this data unless their role requires this.

SERTUS™

Data Protection Policy

Key Requirements

1. Deal fairly

We may only collect or use personal data if we do so for a legitimate reason and tell the individual concerned what we are doing with their data (e.g. by privacy notices on customer and employee forms, employee handbooks and websites).

A legitimate reason includes where we:

a. have the consent of the individual concerned;
b. are doing so for legitimate business interests (having balanced these against any detriment to the individual);

or

c. need to do so to comply with laws (e.g. employment laws) or a contract with that individual

2. Limit use

Personal data must be used only for the purposes for which it was collected. This means that we should not use data for any purpose which we have not informed the individual about or which would not be obvious to that individual.

3. Don't collect more than is required

The personal data we collect must be adequate, relevant and limited to what is necessary in relation to the purposes for which it was collected. We should not ask for more personal data than we need for the legitimate purpose for which we are collecting it.

4. Keep up-to-date

Personal data must be accurate and kept up-to-date. We should encourage individuals to inform us of any changes to their information (and update our records accordingly). We should not use personal data we suspect might be out-of-date without confirming its accuracy.

5. Don't keep for too long

Personal data should not be kept for longer than is required in order to meet the legitimate purpose for which it was collected. It should then be securely deleted. This requirement is subject to other laws and obligations that require us to retain information for certain periods (e.g. retention of financial or tax records).

6. Respect individuals' rights

Individuals have a number of rights under data protection laws which we must respect. These include rights to:

a. request copies of their personal data held by us;
b. receive copies of personal data originally provided by them in a commonly used, open format;
c. ask us to correct any inaccurate data;
d. ask us to delete or restrict our use of personal data; and
e. object to the use of their data

Data Protection Policy

7. Keep secure

Personal data needs to be kept and used securely. This applies to our information systems, sites, and our day-to-day handling of personal data. The Sertus Information Security Policy sets out the information security requirements that apply across Sertus and advice on site security can be obtained from Sertus.

8. Assess and monitor third parties

Before appointing a third party to collect, store or use personal data for us we must satisfy ourselves that they will act in accordance with the requirements of this policy. As part of this, we must put in place a written contract with them that requires this.

9. Check before transferring outside Europe

We may only give someone outside the European Economic Area (including data hosting providers) access to or a copy of personal data if we follow certain precautions. You should speak to your Data Protection Coordinator before allowing any transfers.

10. Embed and Demonstrate compliance

We must embed the protection of personal data in our business, including through appropriate governance. As part of this, we must perform data protection impact assessments to identify and address privacy risks when we consider new initiatives or processes, or commission new systems, that involve the processing of personal data. We must also be able to demonstrate compliance to regulators, including maintaining core documents about our data handling.

General Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers
- Sertus will provide training to all employees to help them understand their responsibilities when handling data
- Employees should keep all data secure by taking sensible precautions and following the guidelines below
- In particular, strong passwords must be used, and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the company or externally
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

Data Protection Policy

When data is stored **on paper**, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer
- Data printouts should be shredded and disposed of securely when no longer required

When data is stored **electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service
- Servers containing personal data should be sited in a secure location, away from general office space
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones
- All servers and computers containing data should be protected by approved security software and a firewall

Data use

Personal data is of no value to Sertus unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers – always access and update the central copy of any data

Data accuracy

The law requires Sertus to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Sertus should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets
- Staff should take every opportunity to ensure data is updated (for instance, by confirming

a customer's details when they call)
- Sertus will make it easy for data subjects to update the information Sertus holds about them
- Data should be updated as inaccuracies are discovered
- It is the Marketing Manager's responsibility to ensure marketing databases are checked against industry suppression files every six months

Subject Access Request

All individuals who are the subject of personal data held by Sertus are entitled to:

- Ask what information the company holds about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made initially by email addressed to the data controller at dataprotection@trustsertus.com. The individual must then identify themselves in person with original means of identification. Identification via email is not suitable. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always require verification of the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Sertus will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Sertus aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. (This is available on request. A version of this statement is also available on the company's website).

SERTUS™

Data Protection Policy

Training

Sertus recognises the importance of training employees, contractors and temporary staff who regularly use personal data on our behalf. Mandatory training will be provided but you should contact your Data Protection Coordinator if you require further guidance.

Third Party Processors

Our carefully selected partners and service providers may process personal information about you on our behalf as described below:

Digital Marketing Service Providers

We periodically appoint digital marketing agents to conduct marketing activity on our behalf, such activity may result in the compliant processing of personal information. Our appointed data processors include:

- Prospect Global Ltd (trading as Sopro) Reg. UK Co. 09648733. You can contact Sopro and view their privacy policy here: http://sopro.io. Sopro are registered with the ICO Reg: ZA346877. Their Data Protection Officer can be emailed at: dpo@sopro.io

Signature: 

Position: Managing Director

The person who takes overall responsibility for Policy is Shane White, Managing Director.