Centinel Spine GDPR Privacy Policy

1. Introduction

At Centinel Spine, we collect, store and process Personal Data about individuals such as employees, suppliers and other third parties (“Data Subjects”) for a variety of purposes.

This policy outlines how we seek to protect such Personal Data. It helps ensure that we understand the principles governing the use of Personal Data. It also describes how we collect, handle and store Personal Data to meet our own Data Protection standards, and to comply with the EU General Data Protection Regulation 2016/679 (the "GDPR") and other related regulations and delegated national legislation (together "Data Protection Law")**.**

a. Scope

This policy applies to all Employees who handle the Personal Data of individuals for business purposes both inside and outside of Centinel Spine.

b. Objective

Our objective is to protect the data subjects by obtaining, collecting, handling, and processing their Personal Data in accordance with applicable data protection law.

c. Consequences of breaching this policy

We take compliance with this policy and our obligations under Data Protection Law very seriously. A failure to do so may put our employees, others, and Centinel Spine at risk of non-compliance. Any breach of this policy may result in disciplinary action being taken, up to and including dismissal.

d. Related policies and procedures

This policy supplements our other related policies and procedures (which may be implemented or amended from time to time).

e. What is data protection and why is it important?

All individuals have rights pertaining to the way in which their Personal Data are processed. The term "Data Protection" in this policy refers to the processing of Personal Data, the corresponding rights to privacy which Data Subjects have and the legal protection surrounding Personal Data (according to GDPR).

f. What are Personal Data

Personal Data means any data (or a combination of data) from which a living individual can be identified directly or indirectly. Personal Data can be factual, or it can be an opinion about an individual, their actions and behaviour.

Within Personal Data there is a sub-category: **Special Categories of Personal Data:** These are Information related to a person's race or ethnicity, political opinions, religious, spiritual or philosophical beliefs, trade union membership, physical or mental health, sexual life, biometric data for the purpose of uniquely identifying a natural person, genetic data and data concerning a natural person's sex life or sexual orientation (according to Art. 9 GDPR). There are even stricter conditions for processing special categories of Personal Data.

2. Data protection principles

There are a number of principles under the GDPR which must be satisfied while processing Personal Data. In the following chapter you will find a description of how we aim to achieve compliance with these principles:

- **Accountability**: We are responsible for ensuring and must be able to demonstrate that the key principles and rules of Data Protection Law are met.
- **Lawfulness, Fairness and Transparency:** Personal Data may only be processed lawfully, fairly and in a transparent manner. This means we inform Data Subjects on how and why we process their data (transparency) that the processing must match the description given to the Data Subjects (fairness) and that the processing uses one of the legal bases set forth in the GPDR (lawfulness).
- **Purpose Limitation:** We must specify exactly what the Personal Data we collect will be used for (prior to collecting them) and limit the processing of that Personal Data to only what is necessary to meet the specified purpose.
- **Data Minimisation:** The Personal Data we collect shall be adequate, relevant and limited only to what is necessary for the purposes for which they are processed.
- **Accuracy:** We have processes in place to ensure that Personal Data is accurate and kept up to date.
- **Storage Limitation:** Personal Data shall be kept in such a way which enables us to identify the Data Subject for no longer than is necessary for the purposes for which the Personal Data are processed.
- **Security/Integrity and Confidentiality:** We use appropriate technical and organisational measures to protect the integrity and confidentiality of Personal Data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

a. Accountability

Monitoring

We strive to process all Personal Data in accordance with our legal obligations and the principles of Data Protection.

We do reviews on a regular basis and follow the rules of the PDAC Cycle (Plan-Do- Act-Check) for the control and continuous improvement of our processes.

This is to establish that an adequate level of compliance is being achieved.

Personal data breach reporting

It is our responsibility to report a personal data breach to the appropriate supervisory authority within 72 hours, if required by law (this is counted from the time we became aware of the incident). When it is suspected that a Personal Data Breach has taken place for which we are responsible (as Controllers) it will be investigated internally by our Privacy Officer. If the incident results in a risk for Data Subjects, it will be reported to the applicable supervisory authority within 72 hours (of becoming aware of the incident).

Training
All Employees complete Data Protection training relevant to their position.

Our training team ensures that new joiners receive training as part of the onboarding process. Further training is provided on a periodic basis or at a minimum whenever there is a substantial change in the law or our policy and procedure.

Responsibility
Each Employee who handles Personal Data has a responsibility to handle and process the Personal Data in line with this policy and the GDPR.

There are positions in Centinel Spine with specific areas of responsibility:

- **The Leadership Team** is ultimately responsible for ensuring that we meet our legal obligations.
- **The International Team** has overall responsibility for ensuring employees in the EU comply with Data Protection Law.
- **The Privacy Officer** has overall responsibility for the day-to-day implementation of this policy and for**:**
    - Reviewing all Data Protection procedures and policies on a regular basis
    - Arranging Data Protection training and advice for all staff members and those included in this policy
    - Responding to Data Subjects who wish to know which Personal Data are being held on them by us
    - Checking and approving with third parties that handle our Personal Data and contracts or agreements regarding Processing
    - Maintaining a record of Processing activities including regular reviews and approvals
- **The Head of Information Systems** is responsible for:
    - Ensuring that 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 Centinel Spine is considering using to retain or process Personal Data

Overview over processing activities
The GDPR (Art. 30) stipulates broad requirements regarding the documentation and proof of compliance with Data Protection obligations. A key element in this regard is the overview over processing activities as set forth in Art. 30 GDPR. We demonstrate GDPR compliance through documentation of processes.

“Privacy by design”
We seek to structure internal processes to have Data Protection principles embedded into every stage of Processing activities. “Privacy by design” means that, both before and during any Processing activity we carry out, we must implement appropriate technical and organisational measures to integrate safeguards into the Processing. This is important in order to protect Data Subjects and meet the requirements of the GDPR.

We always aim to implement appropriate technical and organisational measures both at the time of determination of the means for Processing and at the time of the Processing itself in order to ensure the principle of Data Minimisation is met.

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, a pre-Data Protection Impact Assessment (DPIA) check must be completed before starting a project (a preliminary, shorter Data Protection Impact Assessment). Depending on the outcome, a full DPIA might be conducted.

b. Lawfulness, fairness and transparency

We are responsible for understanding the context in which the Personal Data processing occurs as part of our day-to-day operations. We want to ensure that this is done fairly and in line with the law, and that we can clearly describe this to Data Subjects.

We will always process Personal Data lawfully, fairly, and transparently in accordance with the Data Subject's rights.

The GDPR also designates obligations on our third-party suppliers/contractors that process Personal Data on our behalf. Under the GDPR, we are legally required to:

- only engage the services of third-party suppliers/contractors who can demonstrate compliance with the GDPR;
- put in place prescribed contractual arrangements with third party suppliers/contractors which meet the requirements of the GDPR; and
- demonstrate to the data protection authorities that we have complied with these legal obligations.

Personal data collection and notification
We may only collect Personal Data where it is necessary for lawful purposes or explicitly allowed. We will only collect Personal Data from Data Subjects if one of the following statements applies:

- We are required to do so by an obligation imposed on us by EU or applicable local law.

  The processing is necessary to do so for business purposes and for our organisation to enter into or perform its contractual obligations with Data Subjects;
- The processing is in our (reasonable) legitimate interests and the data subjects do not have more important conflicting interests;
- The individuals consented. This consent needs to be freely given and to be gathered according to the rules in Art. 7 GDPR.

- The data processing is in the vital interest of the data subject or another person.

When we collect personal data, we provide Data Subjects with information regarding the processing of their personal data free of charge in a concise, transparent, intelligent, and easily accessible form, using clear and plain language.

c. Purpose limitation: Processing for limited purposes

Personal Data collected for one purpose may not usually be used for a different purpose.

We aim to only process Personal Data for purposes specifically permitted under GDPR. We inform the Data Subjects of those purposes.

d. Data minimization: Adequate, relevant and non-excessive processing

Every processing should only use as much Personal Data as is required to successfully accomplish a particular purpose.

We will always seek to collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject, and do not collect Personal Data which we do not need.

e. Accuracy: Ensuring that personal data is accurate

We aim to ensure that our systems and processes for identifying inaccurate information are robust and to act quickly to update or erase any inaccurate Personal Data.

We endeavour to ensure that the Personal Data we hold is accurate and kept up to date.
The Data Subjects may ask that we correct inaccurate Personal Data relating to them.

f. Storage limitation: Timely processing and data retention

We aim to not keep the Personal Data of Data Subjects for any longer than is necessary in accordance with applicable law.

We take all required steps to destroy or erase all Personal Data from our systems (electronic/paper-based) which is no longer required.

g. Security/integrity and confidentiality: Security of personal data

We strive to make sure that all Personal Data held by us are subject to a level of security that is appropriate for the potential risk.
We take appropriate security measures against unlawful and unauthorised Processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

Security procedures include (but are not limited to):

- Entry controls – any stranger seen in entry-controlled areas will be reported.
- Secure lockable desks and cupboards – desks and cupboards are kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).
- Data stored on a computer is protected by strong passwords.
- Data is never saved directly to mobile devices such as laptops, tablets, or smartphones (but to centralized servers).

- Methods of disposal – paper documents are shredded. Digital storage devices are physically destroyed when they are no longer required.

- Equipment – data users ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

3. Rights of the data subject

We strive to respond to any requests from Data Subjects exercising their rights without undue delay, and within one month of receipt. It may only take longer if exceptional circumstances are in place.

Data subjects have the following rights:

- Right to information
- Right to rectification
- Right to deletion
- Right to restriction of processing
- Right to data portability
- Right to object

Data Subjects also have the right to lodge a complaint with the Data Protection supervisory authority about how we process their Personal Data.

4. Data transfers

We sometimes transfer Personal Data to other entities. These entities can be companies within our group of undertakings but also other companies who process data on behalf of our company. Centinel Spine will always ensure that these transfers are based on a legal basis.

,

If we engage companies to process data on our behalf, we will cooperate only with processors who fulfil our requirements of providing appropriate technical and organizational measures which meet our standards and the requirements of data protection law. Before personal data is processed, data processing agreements will be in signed to bind the processor accordingly.

5. Data protection coordinator and Data Protection Officer

The Privacy Officer/ Data Protection Officer helps facilitate our compliance with Data Protection Law and acts as a point of contact for day-to-day issues and questions on Data Protection for both employees and external persons.

The Privacy Officer/ Data Protection Officer has overall responsibility for managing the roll out of the various GDPR project work streams and the day-to-day implementation of this policy. These are her contact details:

Clivetty Martinez | Privacy Officer/ Data Protection Officer
Centinel Spine
900 Airport Road - Suite 3B | West Chester, PA 19380
+1 717.869.4491
c.martinez@centinelspine.com | www.centinelspine.com

The data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data. The data protection officer reports directly to the highest management level.

6. Glossary of Terms

Term	Meaning
Employee(s)	All those employed or engaged in any capacity by Centinel Spine. For the purposes of this policy, the word Employees extends to include the following categories: Board Members, Employees (full time, fixed term, part time and temporary), Contract workers, and pensioners.
Controller	A Controller is a person or organisation that determines the purposes for which, and the manner in which, any Personal Data are processed, establishing practices and implementing policies in line with the GDPR.
Data Protection	This term refers to the relationship between the processing of Personal Data, the associated expectations of privacy and the legal protection surrounding them.
Data Subject	The individual to whom Personal Data relates such as an employee, client, contact person with a business partner, etc.
Data Protection Authority	The Data Protection Commission is the supervisory authority/regulator responsible for enforcing Data Protection Law and upholding the data protection and privacy rights of Data Subjects in relation to the Processing of their Personal Data.
Personal Data	Personal Data means any information (or a combination of information) from which a living person can be directly or indirectly identified as well as information containing statements about a person (e.g., Name, salary information, marital status, sick leave dates)
Personal Data Breach	This is 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.
Processing	Processing is any activity which involves the use of Personal Data. It includes i.e., obtaining, recording, or holding Personal Data, or carrying out any operation or set of operations on Personal Data including organising, amending, retrieving, using, disclosing, erasing or destroying data. Processing also includes sharing or transferring Personal Data to third parties and accessing of Personal Data held by a Controller or Processor.
Processor	A Processor is any organisation or external person that processes Personal Data on behalf of and/or on instruction of a Controller.
Special Categories of Personal Data	As defined in Art. 9 GDPR: Personal Data that are related to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or sexual life/orientation, biometric data for the purpose of uniquely identifying a natural person and/or genetic data.