Effective from 2023-10-15

Data Protection Policy

CarpoNovum AB

Table of Contents

1. INTRODUCTION 3

2. SCOPE AND PURPOSE 3

3. DEFINITIONS 3

4. CATEGORIES OF DATA SUBJECTS 4

4.1. Employees, Board Members, and Consultants 4
4.1.1. Purpose of Processing 4
4.1.2. Types of Personal Data 5
4.1.3. Handling of Personal Data 5
4.1.4. Sharing of Personal Data 7
4.2. Business Operations - Investors, Resellers, Partners, and Other Business Partners 7
4.2.1. Purpose of Processing 7
4.2.2. Types of Personal Data 8
4.2.3. Processing of Personal Data 9
4.2.4. Sharing of Personal Data 9
4.3. Surgeons 10
4.3.1. Purpose of Processing 10
4.3.2. Types of Personal Data 10
4.3.3. Processing of Personal Data 11
4.3.4. Sharing of Personal Data 11
4.4. Patients 12
4.4.1. Purpose of Processing 12
4.4.2. Types of Personal Data 12
4.4.3. Processing of Personal Data 13
4.4.4. Sharing of Personal Data 13
4.5. Other Stakeholders 14
4.5.1. Purpose of Processing 14
4.5.2. Types of Personal Data 14
4.5.3. Processing of Personal Data 14
4.5.4. Sharing of Personal Data 14

5. SECURITY AND PRIVACY 14

6. GENERAL PRINCIPLES 15

6.1. Legality, Fairness, and Transparency 15

6.2. Purpose Limitation **15**
6.3. Data Minimization **15**
6.4. Accuracy **15**
6.5. Storage Limitation **16**
6.6. Integrity and Confidentiality **16**

7. RIGHTS OF DATA SUBJECTS **16**

7.1. Right to be Informed **16**
7.2. Right of Access **16**
7.3. Right to Rectification **16**
7.4. Right to Erasure (Right to be Forgotten) **16**
7.5. Right to Restrict Processing **16**
7.6. Right to Data Portability **17**
7.7. Right to Object **17**
7.8. Right to be Notified **17**
7.9. Rights in relation to Automated Decision Making and Profiling **17**

8. TRANSFER OF PERSONAL DATA TO THIRD PARTIES AND THIRD COUNTRIES **17**

9. COOKIE POLICY **18**

9.1. Introduction **18**
9.2. What are cookies? **18**
9.3. Which cookies do we use? **18**
9.4. How to manage cookies **18**
9.5. Changes to this policy **18**

10. INCIDENT HANDLING AND DATA BREACHES **19**

10.1. Incident Handling **19**

11. CHANGES IN THE DATA PROTECTION POLICY **20**

12. CONTACT INFORMATION **20**

Effective from 2023-10-15

1. Introduction

This document constitutes CarpoNovum's (the company's) Data Protection Policy, designed to ensure responsible and secure handling of personal data in accordance with applicable legislation, such as the European Union's General Data Protection Regulation (GDPR). The policy applies to all employees and subcontractors within the company and encompasses all activities where personal data is collected, stored, used, and shared.

The Data Protection Policy is a crucial part of the company's commitment to protect personal data and maintain integrity. By adhering to this policy, the company ensures it meets legal requirements, minimizes risks associated with its personal data processing activities, builds trust with customers, employees, and other stakeholders, and educates and informs employees about data protection principles and best practices.

This policy describes the company's commitments and guidelines for handling personal data, as well as the measures taken to ensure compliance. The policy covers key aspects such as data protection principles, rights of the data subject, information management, and roles and responsibilities within the organization. The policy is designed to be clear and easily understandable, and is regularly updated to align with legislation and best practices in data protection.

The policy is based on the various categories of individuals ("data subjects") for whom the company processes personal data. This approach allows the reader to quickly identify the information relevant to them.

2. Scope and Purpose

This Data Protection Policy applies to all employees, subcontractors, consultants, and third parties who process personal data on behalf of the company. The purpose of this policy is to ensure that the company and all involved parties handle personal data in a lawful, accurate, and transparent manner, in line with applicable data protection legislation, such as the European Union's General Data Protection Regulation (GDPR) and national data protection laws.

3. Definitions

To clarify the meaning of various terms and concepts used in this Data Protection Policy, below is a list of definitions according to the GDPR:

Data Subject: A natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person (Article 4.1).

Personal Data: Any information relating to an identified or identifiable natural person, such as name, address, email address, phone number, personal identification number, IP address, and photographs (Article 4.1).

Processing: Any operation or set of operations performed on personal data, such as collection, storage, alteration, transmission, deletion, and use (Article 4.2).

Data Controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data and is responsible for complying with data protection legislation (Article 4.7).

Data Processor: The natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller and in accordance with their instructions (Article 4.8).

Third Party: A natural or legal person, public authority, agency, or body other than the data subject, data controller, data processor, or persons who are under the direct authority of the data controller or data processor (Article 4.10).

Consent: The data subject's freely given, informed, and unambiguous indication by means of a statement or clear affirmative action, by which the data subject signifies agreement to the processing of his or her personal data (Article 4.11).

Sensitive Information (Special Categories of Personal Data): Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for the unique identification of a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. These categories of personal data are considered more sensitive than others and are subject to special protection (Article 9).

4. Categories of Data Subjects

This policy is divided into sections based on the different categories of data subjects for whom the company processes personal data.

4.1. Employees, Board Members, and Consultants

4.1.1. Purpose of Processing

The primary purpose of processing is to enable payment of compensation for work, to fulfill the company's obligations as a contracting party and employer, and to ensure a safe and secure working environment. The processing is a prerequisite for many essential activities within the company:

1. **Payroll Administration**: To ensure the correct payment of salaries and management of benefits, this processing is based on the performance of a contract (Article 6.1 b).

2. **Employment Administration**: To manage employment terms, such as employment contracts, vacation, sick leave, and parental leave, this processing is based on the performance of a contract (Article 6.1 b).

3. **Staff Development and Training**: To offer training, skills development, and career opportunities, this processing is based on the company's legitimate interests (Article 6.1 f).

4. **Work Environment and Safety**: To ensure a safe and healthy working environment and to comply with workplace safety legislation, this processing is based on the company's legal obligation (Article 6.1 c).

5. **Performance Evaluation and Feedback**: To evaluate and provide feedback on employees' performance and contribute to their personal and professional development, this processing is based on the company's legitimate interests (Article 6.1 f).

6. **Internal Communication and Collaboration**: To facilitate effective communication and collaboration between employees and departments, this processing is based on the company's legitimate interests (Article 6.1 f).

4.1.2. Types of Personal Data

The company collects and processes the following types of personal data for employees, board members, and consultants, to the extent necessary to fulfill the company's commitments:

1. **Identification Data**: Name, personal identification number, address, phone number, email address, and possibly photographs.

2. **Employment-Related Data**: Employment date, type of employment (permanent, temporary, or consultancy contract), job description, title, department, supervisor, salary, and employment history.

3. **Education and Competence Data**: Educational history, degrees, certificates, licenses, skills, language proficiency, and possibly references.

4. **Banking and Tax Data**: Bank account number, tax class, and potential tax declarations.

5. **Benefits and Insurance Data**: Pension plan, insurances, benefits, and compensations.

6. **Attendance and Time Reporting**: Working hours, absences, vacations, sick days, and overtime.
    a. **Sensitive Personal Data**: Health-related data (e.g., reasons for illness, medical certificates).

7. **Performance and Evaluation Data**: Work performance, objectives, evaluations, feedback, and potential disciplinary actions.

8. **IT and Communication Data**: Usernames, passwords, email correspondence, IP addresses, and logs of usage of the company's IT systems and resources.

9. **Security Data**: Access and security checks, potential security incidents, and violations.

4.1.3. Handling of Personal Data

For staff, board members, and consultants, we collect personal data in the following ways for the different types of information:

Effective from 2023-10-15

1. **Identification Data**: Collected through employment contracts, consultancy agreements, and/or other relevant documents that the employee/consultant completes upon employment or the commencement of the assignment. It may also include collecting photographs during company events or for use on the company's internal platforms.

2. **Employment-Related Data**: Collected upon hiring through employment contracts, introductory meetings, and potentially during follow-up meetings with managers. Sensitive personal data, such as trade union membership, may be collected upon employment if the employee explicitly consents.

3. **Education and Competence Data**: Collected by the employee/consultant providing relevant documents, such as diplomas and certificates, and through self-reporting of skills and language proficiency upon employment or during competence development discussions.

4. **Banking and Tax Data**: Collected upon hiring by the employee/consultant completing the necessary documents for payroll and tax reporting.

5. **Benefits and Insurance Data**: Collected upon employment or during changes in benefit and insurance plans, by the employee/consultant completing relevant documents and/or participating in benefits discussions.

6. **Attendance and Time Reporting**: Collected by the employee/consultant reporting work hours, absences, and vacations via time reporting (email) and/or invoicing to the company's financial firm. Sensitive personal data, such as health-related data, is collected when the employee/consultant submits sick leave certificates or other medical documents.

7. **Performance and Evaluation Data**: Collected through regular performance discussions and evaluations with managers, feedback from colleagues, and potentially by the employee/consultant self-reporting their work performances and objectives. Typically, such information is shared verbally, but it may be documented in certain cases.

8. **IT and Communication Data**: Collected automatically through the use of the company's IT systems and resources, for instance, by logging into the work computer, sending emails, and using the company's network and applications.

9. **Security Data**: Collected by the employee/consultant participating in security checks, such as using access cards or biometric identification upon entry. Sensitive personal data, like biometric information, is collected when the employee/consultant gives explicit consent and when necessary for security purposes. This might also involve security incidents and violations reported by the employee, colleagues, or security staff.

The company stores such personal data on its server with limited access, in Microsoft 365, as well as in locked cabinets for physical documents. Additionally, some data is managed by the company's auditing and accounting firm, which uses secure and encrypted systems. (See below "Sharing of Personal Data").

4.1.4. Sharing of Personal Data

The company may share personal data with external parties when necessary to fulfill its obligations as an employer, to provide employees and consultants with services and benefits, or to maintain the company's security and operations.

When we share personal data with external parties, we ensure that these parties handle the data in accordance with the GDPR and other relevant data protection laws. We enter into data processing agreements with all external parties that process personal data on our behalf to ensure they adhere to our guidelines and requirements regarding data protection. Examples of external parties with whom we might share personal data include:

1. **Auditing and Accounting Firms**: We may share banking and tax data as well as employment-related data with our auditing and accounting firm to ensure accurate salary payments and tax deductions.

2. **Insurance Companies and Pension Administrators**: We may share personal data with insurance companies and pension administrators to manage insurances and pensions for our employees and consultants.

3. **IT Providers and Support Companies**: We may share IT and communication data with IT providers and support companies to ensure that our IT systems and resources operate correctly and securely. This includes data processing in Microsoft 365.

4. **Authorities**: We may share personal data with authorities when legally required to do so, for example, to report incomes and taxes to the Tax Agency.

We only share personal data with external parties when necessary and in compliance with applicable laws. We take appropriate measures to ensure that the shared information is limited to what is required for the purpose of sharing and that the data is protected in the best possible way.

4.2. Business Operations- Investors, Resellers, Partners, and Other Business Partners

4.2.1. Purpose of Processing

The company processes personal data for investors, suppliers, partners, and other business partners with the aim of maintaining and developing business relationships and ensuring efficient and professional communication. The primary purposes for processing these personal data include:

1. **Business Administration**: We process personal data to administer and manage purchase orders, invoices, contracts, and other business transactions between us and our business partners. This processing is based on the company's obligation to fulfill a contract (Article 6.1 b) and the company's legitimate interests (Article 6.1 f).

2. **Communication**: We use contact details to communicate with our business partners, such as sending information about products, services, projects, and partnership opportunities, and to inform our investors about the company's performance, future prospects, key events, and financial position. This processing is based on the company's

legitimate interests (Article 6.1 f) in maintaining and developing business relationships and informing investors.

3. **Project and Quality Management**: We process personal data to monitor and coordinate projects, including identifying and documenting participation in project groups and steering groups, and ensuring that our quality system meets internal and external requirements. This processing is based on the company's legitimate interests (Article 6.1 f) to ensure projects and quality systems meet standards.

4. **Supplier and Customer Management**: We process personal data to maintain and update supplier and customer lists and to evaluate and monitor performance and quality in our business relationships. This processing is based on the fulfillment of a contract (Article 6.1 b) and the company's legitimate interests (Article 6.1 f) in maintaining business relationships.

5. **Legal and Regulatory Obligations**: We process personal data to meet our legal and regulatory obligations, such as complying with accounting, tax, and reporting laws to authorities and rules related to investor relations and securities markets. This processing is based on the company's obligation to comply with laws and regulations (Article 6.1 c) and the company's legitimate interests (Article 6.1 f).

6. **Security and Privacy**: We process personal data to ensure our systems and processes are secure and to protect the personal integrity of those involved in our business relationships. This processing is based on the company's legitimate interests (Article 6.1 f) in ensuring the security of the company's systems and processes and protecting personal privacy.

By processing personal data for these purposes, the company ensures an efficient and professional business operation and maintains good business relationships with our investors, resellers, partners, and other business partners.

4.2.2. Types of Personal Data

For investors, suppliers, collaborators, and other business partners, the following types of personal data may be processed:

1. **Identification Data**: Name, title or position, phone number, and email address.

2. **Contact History**: Communication, meeting notes, email correspondence, and other interactions with the registered individual.

3. **Investment-related Data**: Investment amounts, ownership stakes, and investment history.

4. **Bank and Financial Data**: Bank account numbers and payment information for individuals representing the company or investor.

5. **Compliance and Security Data**: Data required to comply with laws, regulations, and provisions, for instance, within the framework of anti-money laundering, market abuse, and insider trading. This may include social security numbers or other identification information required to conduct necessary checks.

4.2.3. Processing of Personal Data

To fulfill obligations towards investors and business partners, certain personal data is collected and processed. This data is gathered in the following manner:

1. **Identification Data**: This data is collected from investors and business partners when contact is established, agreements or collaborations are entered into, or when they participate in activities. The data might be collected via email, phone, contracts, meetings, web forms, or other communication channels.

2. **Contact History**: This information is collected during communication between the parties through meetings, phone calls, emails, or other forms of interaction.

3. **Financial Data**: This data is gathered in connection with financial transactions, investments, and payments, as well as when reporting to authorities.

4. **Legal and Regulatory Data**: This data is collected by obtaining and reviewing relevant documents, such as contracts, certificates, and reports, to ensure compliance with laws and regulations.

5. **Benefits and Insurance Data**: This information is gathered by obtaining and reviewing contracts, insurance policies, and other documents related to benefits and insurances that may be associated with investments or collaborations.

The company stores personal data for investors, resellers, collaborators, and other business partners in its quality system on the company's server as well as in Microsoft 365.

4.2.4. Sharing of Personal Data

When necessary to fulfill obligations towards investors, resellers, collaborators, and other business partners, personal data may be shared with external parties. This sharing occurs only in accordance with applicable legislation and to ensure commitments are fulfilled. Examples of such sharing include:

1. **Third-party Providers**: Personal data may be shared with third-party providers, such as legal advisors, auditors, IT providers, payment intermediaries, and other service providers, to fulfill obligations towards investors and business partners. This includes processing in Microsoft 365.

2. **Authorities**: In some cases, it may be necessary to share personal data with authorities, such as tax agencies, financial supervisory authorities, or other regulatory bodies, to meet legal requirements, reporting obligations, or to ensure compliance with rules and regulations.

3. **Potential Business Partners**: When negotiations or discussions about potential business collaborations, investments, or sales are conducted, personal data may be shared with

potential business partners. In these cases, only necessary data is shared, and confidentiality agreements are entered into before the sharing occurs.

4. **Other Parties**: It may sometimes be necessary to share personal data with other parties, such as banks, insurance companies, or other financial institutions, to ensure proper management of investments, payments, and insurance matters.

4.3. Surgeons

4.3.1. Purpose of Processing

The company processes personal data for surgeons with the purpose of ensuring that only accredited surgeons use the company's medical products during surgical procedures, as well as to improve and further develop the company's products. The processing of personal data for surgeons aims to:

1. **Fulfill Contracts**: The processing of personal data is necessary to fulfill contractual obligations between the company and the surgeons. By ensuring that only accredited surgeons access and use the company's products, a high standard of quality and patient safety is maintained. This processing is based on Article 6.1(b).

2. **Protect Individual's Interest**: By maintaining a list of accredited surgeons, the company can ensure that surgeons have the competence and experience required to use the company's medical products safely and effectively. This protects both the surgeons' and the patients' interests and contributes to raising the quality of surgical procedures. This processing is based on Article 6.1(d).

3. **Legal Basis**: The company is obligated to maintain information about the use of the company's medical products to fulfill regulatory requirements. This processing is based on Article 6.1(c).

The company processes surgeons' personal data to manage customer surveys, expressions of interest, participation in workshops, and the accreditation process for surgeons wanting to use the company's products. By collecting and storing this data, the company can effectively and correctly administer accreditations and ensure that only qualified surgeons use the company's medical products.

4.3.2. Types of Personal Data

To achieve the stated purposes of processing, the company collects and processes the following personal data for surgeons:

1. **Identification Data**: This includes the name and the hospital where the surgeon works, as well as contact details. These details are used to ensure that only accredited surgeons access and use the company's medical products.

2. **Accreditation Data**: Information about the surgeon's accreditation, such as the date of accreditation, certificates, and any additional training or competencies relevant to the use of the company's products. These details are used to monitor and maintain the

surgeons' competence and ensure they meet the requirements to use the company's medical products.

3. **Education and Workshop Participation**: Information about the surgeon's participation in training, workshops, and other events linked to the company's medical products and the accreditation process. This data is used to track the surgeon's training history and ensure they receive relevant and adequate training to use the company's products.

4. **Product Evaluation**: Information about the surgeon's opinion of the company's products. This data is used to better understand the use of the company's products, allowing the company to develop and improve them.

4.3.3. Processing of Personal Data

Surgeons' personal data is collected in the following ways:

1. **Direct Communication**: The data is obtained directly from the surgeons themselves, for example, by filling out forms, participating in training or workshops, or through email communication with the company.

2. **Hospitals and Clinics**: Details about the surgeons' employment and accreditation can also be collected from the hospitals and clinics where the surgeons work. This might include verifying their employment or checking they have undergone the necessary training and accreditation to use the company's medical products.

3. **Training and Workshops**: When surgeons participate in training or workshops organized by the company, some personal data is collected to document their participation, progress, and any certifications.

4. **Customer Surveys**: When surgeons use the company's products, they may be asked to complete a customer survey where they inform the company about their opinions on the company's products.

The collected personal data is stored in the company's quality system and on its server, as well as in Microsoft 365.

4.3.4. Sharing of Personal Data

In the case of surgeons, personal data may be shared with relevant parties in accordance with applicable laws and the company's policy. This may include the following situations:

1. **Hospitals and Clinics**: Personal data may be shared with the hospitals and clinics where the surgeons work to ensure that these surgeons are accredited and qualified to use the company's medical products.

2. **Authorities and Regulatory Bodies**: In certain cases, it may be necessary to share personal data with authorities and regulatory bodies, for example, in connection with supervision, inspection, or to fulfill legal requirements.

3. **External Training and Certification Bodies**: If the company collaborates with external organizations to provide training and certification to surgeons, personal data might be shared with these organizations for the purpose of administering and documenting trainings and certifications.

4. **Other Third-Party Providers**: The company might employ other data processors to process personal data, for example, providers of IT services or cloud-based storage solutions. In such cases, it is ensured that the data processors follow the company's policy and applicable laws regarding the processing of personal data. This includes Microsoft 365.

The company takes the necessary measures to ensure that all parties accessing personal data handle them responsibly and securely, in accordance with applicable laws and the company's policy on personal data processing.

4.4. Patients

4.4.1. Purpose of Processing

The company processes personal data of patients to ensure the performance, efficiency, and safety of the products, as well as to continually improve and adapt the products according to the needs of patients and caregivers. Furthermore, the company fulfills its legal and regulatory obligations, such as adhering to laws and regulations in medical technology, health care, and reporting to authorities. The legal basis for this processing under the GDPR includes the protection of patients' interests (Article 6.1 d), legal obligations within health care (Article 9.2 h), and the company's obligation to comply with the law (Article 6.1 c).

4.4.2. Types of Personal Data

The company processes several types of personal data for patients undergoing surgery with the company's products, including:

1. **Identification Data**: such as name, personal identification number, and contact details (phone number and email address).

2. **Health-related Data**: such as medical history, diagnoses, treatment plans, surgical procedures, medical equipment used, and any side effects or complications.

3. **Demographic Data**: such as age, gender, and ethnicity, which can help the company identify any differences in treatment outcomes between different patient groups.

4. **Administrative Data**: such as the date of the operation, caregiver, surgeon, and possibly the care team involved in the patient's treatment.

5. **Communication Data**: such as notes from calls or meetings between the patient and medical personnel, and any correspondence between the company and the caregiver regarding the patient's treatment.

4.4.3. Processing of Personal Data

The company collects personal data about patients undergoing surgery with the company's products in several ways:

1. **Directly from Care Providers**: The company may receive personal data directly from care providers and surgeons who use the company's products in the treatment of patients. This data may include medical history, diagnoses, treatment plans, as well as details about surgical procedures and the use of medical equipment.

2. **Indirectly from Other Sources**: In some cases, the company may obtain personal data about patients indirectly from other sources, such as medical records, research studies, or clinical trials. This data is used to analyze and improve product performance, safety, and efficiency.

3. **From the Patient Themselves**: Patients may sometimes choose to provide personal data directly to the company, for instance, by participating in surveys, patient associations, or by sharing their experiences and views about the company's products.

Patient data is stored in the Webdoc system, which is only accessible by the business manager and assistant via BankID.

4.4.4. Sharing of Personal Data

The company may share patients' personal data with various parties in accordance with applicable laws and regulations and to fulfill its commitments to patients and caregivers. Such sharing of personal data may include:

1. **Care Providers and Medical Personnel**: Patient information may be shared with the care providers and medical personnel involved in the patient's care and treatment to ensure the correct use of the company's medical products and to enable effective communication between caregivers, patients, and the company.

2. **Authorities and Regulatory Bodies**: In certain cases, the company may be required to share patient data with authorities and regulatory bodies, such as the Medical Products Agency, the National Board of Health and Welfare, or the Data Protection Authority (IMY), to fulfill legal requirements or as part of a supervisory process.

3. **Data Processors**: The company may employ data processors to perform certain services, such as IT services, database management, or analytical tools. In these cases, the data processors will process patient data on behalf of the company and only in accordance with the company's instructions and applicable data protection laws.

4. **Research and Development**: To improve and develop the company's products and contribute to medical research, patient information may be shared with research institutions or partners. In these instances, the personal data will be anonymized or de-identified to the greatest extent possible to ensure patients' privacy.

4.5. Other Stakeholders

In addition to the primary categories of registrants mentioned above, the company also collects personal data to a limited extent based on visits to the company's website.

4.5.1. Purpose of Processing

The purpose of processing is to continuously improve and maintain the company's website and to provide visitors with the opportunity to register for activities organized by the company. The processing is based on the company's legitimate interest (Article 6.1 f).

4.5.2. Types of Personal Data

As much as possible, data is anonymized so as not to be traceable to an individual. However, some data is associated with an IP address and is thus considered personal data. The following information is managed:

1. **Anonymous User Data**: This includes data such as the number of visitors, page views, time spent, traffic source, device information, and other general user information that cannot be linked to a specific individual.

2. **IP Addresses**: An IP address can be used to identify a specific device and its location. IP addresses can be personal data, but they are generally treated as anonymous data for understanding the geographical location of visitors.

3. **Cookies**: Cookies are small text files stored on the visitor's device and can be used to track their browser activity and preferences. Some cookies may contain personal data such as name or email address, but they are generally treated as anonymous data.

4.5.3. Processing of Personal Data

Personal data is collected when a person visits the company's website. Information related to the visitor's use of the website is automatically collected. Information for participation in activities organized by the company is entered by the visitor themselves via forms on the website.

4.5.4. Sharing of Personal Data

The company's website is managed by the company Wix, which also collects and stores all statistics related to the website's usage on behalf of the company. The data may also be shared with other third-party providers working on maintaining or developing the company's website.

5. Security and Privacy

The company takes a series of technical and organizational measures to protect personal data from unauthorized access, alteration, dissemination, or destruction. These measures include:

1. **Access Control**: We limit access to personal data to employees who need the information to perform their duties. Access to personal data is only granted after authorization has been approved by the CEO or HR.

2. **Training and Awareness**: We educate our employees in data protection and security routines to ensure that they handle personal data in a secure and responsible manner.

3. **Encryption**: We encrypt sensitive information, such as passwords and banking details, to protect it during transmission and storage.

4. **Backup and Recovery**: We regularly backup personal data to prevent loss or damage to the information. We have procedures to restore lost or damaged information when necessary.

5. **Physical Security**: We store physical documents with personal data in locked cabinets or secure areas accessible only to authorized personnel.

6. **Incident Management**: We have procedures to quickly identify and handle any security incidents involving personal data. In the event of an incident, we will take measures to limit the damage and inform affected individuals and supervisory authorities in accordance with applicable legal requirements.

7. **Regular Review and Update**: We regularly monitor and review our security measures and data protection practices to ensure they are effective and updated according to applicable legislation and best practices.

6. General Principles

The collection of personal data always occurs in accordance with applicable data protection legislation and with respect for the data subject's rights and privacy. When it comes to sensitive personal data, we ensure that we only collect and process this data when it is absolutely necessary and with the consent of the data subject, if required. We adhere to the following general principles when processing personal data:

6.1. Legality, Fairness, and Transparency

All processing of personal data is based on a legal foundation, such as consent from the data subject or the fulfillment of a contract. We always inform the data subject about what type of personal data is being collected, why it is being collected, and how it will be processed. We also ensure that all processing occurs in a fair and transparent manner.

6.2. Purpose Limitation

We only collect personal data for specific and explicitly defined purposes. We do not process personal data in ways that are incompatible with these purposes.

6.3. Data Minimization

The company only collects the personal data that is necessary to fulfill the specified purpose.

6.4. Accuracy

We ensure that personal data processed is accurate and up-to-date. We take appropriate measures to correct or delete inaccurate or outdated personal data.

6.5. Storage Limitation
We store personal data only as long as necessary for the specific purpose and in accordance with applicable laws and regulations. We delete personal data when they are no longer needed for the specific purpose or when the data subject requests it.

6.6. Integrity and Confidentiality
We ensure that processed personal data is protected against unauthorized access, alteration, deletion, or disclosure. We adopt suitable technical and organizational measures to ensure that personal data is handled securely.

7. Rights of Data Subjects
The company respects the rights of the data subjects and strives to fulfill these in accordance with current data protection legislation. Below is a description of the rights a data subject has. Note that when it comes to patient information, the company is subject to several regulatory legal requirements that prevent the destruction of medically significant data.

7.1. Right to be Informed
The data subject has the right to be informed about how their personal data is processed and why. This includes information about which personal data is processed, the purpose of the processing, which categories of recipients can access the data, and how long the data will be stored.

7.2. Right of Access
The data subject has the right to request and gain access to their personal data processed by the company. This includes information about which personal data is processed, where it comes from, and who receives the information.

7.3. Right to Rectification
The data subject has the right to request that incorrect or incomplete data be corrected or supplemented.

7.4. Right to Erasure (Right to be Forgotten)
The data subject has the right to request the deletion of their personal data when they are no longer necessary for the purpose they were collected for or if the processing lacks a legal basis.

7.5. Right to Restrict Processing
The data subject has the right to request that the processing of personal data be restricted if the data is incorrect, the processing is illegal, or if the data subject has objected to the processing.

7.6. Right to Data Portability
The data subject has the right to retrieve and transfer their personal data to another data controller if this is technically possible.

7.7. Right to Object
The data subject has the right to object to the processing of their personal data if the processing is based on a balance of interests and the data subject believes their own interests outweigh the company's interests.

7.8. Right to be Notified
The data subject has the right to be informed of any security breaches that may compromise their personal data. If there is a high risk that the rights and freedoms of individuals are threatened due to a data breach, the company will promptly communicate with the affected individual about the nature of the breach, the likely consequences, and the measures taken to address and mitigate the breach.

7.9. Rights in relation to Automated Decision Making and Profiling
The data subject has the right not to be subject to decisions solely based on automated processing, including profiling, which produces legal effects or significantly affects them. The company ensures that individuals can obtain human intervention, express their point of view, and contest decisions made about them without human involvement.

8. Transfer of Personal Data to Third Parties and Third Countries
The company ensures that all third-party transfers of personal data comply with the GDPR's requirements for the protection of personal data.

For transfers to third countries, the company ensures that the recipient of the personal data in the third country has appropriate safeguards in place. The company conducts an analysis to assess the level of data protection in the recipient country and to assess which measures are adequate to protect data when there is a lack of data protection legislation equivalent to the GDPR. When transferring to a third country where the EU Commission has not reached an agreement on an adequate level of protection, appropriate safeguards as stipulated by the GDPR, such as standard contractual clauses, are used to ensure that the level of protection meets the EU's data protection standards.

The company uses cloud services provided by cloud providers in third countries, primarily Microsoft. The company ensures that cloud providers meet the GDPR's requirements for appropriate safeguards, such as standard contractual clauses or other appropriate safeguards to guarantee that personal data is adequately protected.

The company continuously monitors that all transfers of personal data to third parties, including transfers to third countries, comply with the GDPR requirements. If necessary, appropriate measures are taken to ensure that the law follows data and that personal data is protected in an adequate manner.

Effective from 2023-10-15

9. Cookie Policy

9.1. Introduction

This cookie policy explains how the company uses cookies and similar technologies on our website. By using our website, you consent to our use of cookies in accordance with this policy.

9.2. What are cookies?

Cookies are small text files that are stored on your computer or mobile device when you visit our website. They are typically used to enhance the user experience, for instance, by remembering your settings, tracking your visits to the website, or to display relevant advertisements.

9.3. Which cookies do we use?

We use both first-party cookies (which we set on our own website) and third-party cookies (which are set by other companies). The cookies we use on our website are either essential for the website to operate correctly or to enhance your experience of the website.

The specific cookies used on our website may vary over time, but usually include:

1. **Essential cookies:** These cookies are necessary for the website to function correctly, for example, to remember your settings.

2. **Performance cookies:** These cookies collect information about how visitors use our website, for instance, which pages are visited most frequently, and help us improve our website.

3. **Functional cookies:** These cookies enhance your experience of our website by remembering your choices and preferences, such as language selection and search settings.

4. **Advertising cookies:** These cookies are used to display ads that are relevant to you based on your browsing on our website and other websites.

9.4. How to manage cookies

You can block or delete cookies by changing the settings in your web browser. Please note that if you block cookies, it might affect the functionality of our website and make certain features unavailable.

For more information on how to manage cookies, please visit www.aboutcookies.org or www.allaboutcookies.org.

9.5. Changes to this policy

We reserve the right to change this cookie policy at any time. Any changes will be posted on our website. By continuing to use our website, you consent to such changes.

10. Incident Handling and Data Breaches

The company is responsible for ensuring that all incidents and breaches are managed systematically and correctly to minimize risks to the data subject and the company.

The company's data protection officer is responsible for monitoring and reporting incidents and breaches involving personal data processing to the appropriate authorities. All employees and subcontractors handling personal data are responsible for reporting any incidents or breaches to the company's data protection officer as soon as they become aware of them.

10.1. Incident Handling

1. **Identification of the incident or breach**
   a. All employees and subcontractors handling personal data are obliged to report any incidents or breaches to the company's data protection officer as soon as they become aware of them.
   b. The company's data protection officer is responsible for promptly investigating the incident or breach to assess the extent of any risks to the data subject and the company.

2. **Risk assessment**
   a. The company's data protection officer shall assess the risk to the data subject's rights and freedoms and inform the company management if necessary.
   b. If it is determined that there is a risk to the data subject's rights and freedoms, such as in the event of a significant personal data breach, the company must immediately notify the relevant authorities.

3. **Reporting to the supervisory authority**
   a. If the incident or breach is deemed high-risk or affects a large amount of personal data, the company must report this to the relevant supervisory authorities within 72 hours.
   b. The company's data protection officer is responsible for reporting to supervisory authorities and will provide all necessary information about the incident or breach.

4. **Documentation**
   a. All incidents or breaches reported must be documented by the company's data protection officer, including a description of the event, the personal data affected, the risk assessment, measures taken, and reporting to the supervisory authority.
   b. The documentation must be retained in accordance with the company's archiving policy.

5. **Feedback and measures**
   a. After the incident has been managed and documented, the company should evaluate how the incident could occur and what measures have been taken to handle it. The purpose is to identify areas of improvement and measures to reduce the risk of similar incidents in the future.

The company regularly updates its incident handling plan to ensure it remains current and follows the latest guidelines and requirements of data protection legislation.

11. Changes in the Data Protection Policy

The company reserves the right to change or update this data protection policy at any time. Changes will be posted on the company's website, and the latest version will always be available for review. To ensure the data subject is aware of any changes, it is recommended that the data subject regularly reviews this data protection policy.

If significant changes are made in the processing of personal data, such as a change in the purpose of the processing or a change in the data subject's rights, the company will notify the data subject of these changes in advance, if appropriate.

12. Contact Information

If you have any questions or comments regarding the company's processing of personal data or this data protection policy, please feel free to contact us. You can reach us at: info@carponovum.com

If you are not satisfied with the initial contact, you can turn to The Swedish Authority for Privacy Protection (IMY) at https://www.imy.se for further guidance and help with your questions or complaints regarding our processing of your personal data.