DATA PROTECTION POLICY

Issued by:
Group Compliance Manager

Issued on: January 2024

Version: 1.0

This policy has been approved by the Executive Board of C. Steinweg Group

C. Steinweg Group

TABLE OF CONTENTS

1	AIM OF THE DATA PROTECTION POLICY	3
2	POLICY SCOPE	4
3	DATA PROTECTION PRINCIPLES	5
4	EMPLOYEE FAIR USE POLICY	9
5	DATA TRANSFER POLICY	16
6	THIRD PARTY SERVICE PROVIDERS	17
7	BREACH MANAGEMENT	17
8	TEAM	18

1 Aim of the Data Protection Policy

This data protection policy ("Policy") confirms the commitment of C. Steinweg Group and all of its affiliated companies including without limitation its affiliates located in the European economic area (jointly "Steinweg" or "the Company") to:

- Comply with data protection laws and follow best data protection practices
- Protect the rights of Steinweg's employees, customers and partners
- Be transparent about how Steinweg processes personal data
- Protect its business, employees, customers and partners from the risk of data breaches

Steinweg is committed to safeguard compliance with Data Protection Regulations as a part of a sustainable and accountable approach to business.

In carrying out its operation, Steinweg collects, handles and stores information, some of which directly or indirectly relates to identifiable individuals. This information is referred to as personal data.

This Policy describes how personal data must be collected, handled, stored, disclosed and otherwise "processed" to meet Steinweg's data protection standards and to comply with all applicable national and supranational privacy laws, including in particular the European General Data protection Regulation and its national implementation laws (jointly the "GDPR") In this respect it must be noted that the law(s) applicable with respect to a certain data subject will in any case include the law of the country of residence of the data subject.

Steinweg regards the lawful and correct treatment of personal data as integral to its successful operations and crucial to maintain the confidence of clients, employees and any other parties Steinweg may work with.

This Policy has also been adopted in order to establish essential knowledge and awareness across this Company regarding data protection and privacy issues.

2 Policy Scope

This Policy applies to all employees and any other parties such as customers and partners who have access to any personal data held by or on behalf of Steinweg.

For the avoidance of doubt, any references to “employees” shall include employees, officers, consultants, contractors, casual workers and agency workers as well as directors whether executive or non-executive.

All employees are obliged to ensure that they are aware of and have understood the content of this Policy and their related rights and responsibilities.

The management of Steinweg is confident that you support our commitment to safeguarding your privacy and those of others!

3 Data Protection Principles

This section demonstrates the principles in accordance with the GDPR on how Steinweg's processes individuals' personal data.

A. Lawfulness, fairness and transparency
Steinweg will only process personal data fairly, transparently and lawfully. An individual's personal data must not be processed unless there are lawful grounds for doing so and data subjects must be informed as to how and why their personal data is being processed either upon or before collecting it. Steinweg is transparent with regard to the way it processes personal data and informs employees and other data subjects via its privacy and fair use notices.

Non-Sensitive Personal Data
Steinweg will only process personal data if the purpose of the processing satisfies one of the lawful grounds permitted. Such grounds for non-sensitive personal data are typically:

- Where the processing is necessary for the performance of a contract to which a data subject is a party;

- Where the processing is required by law or other regulation which Steinweg is subject to, such as tax laws and regulations (for example where it concerns the processing of a national identification number;

- Where Steinweg has a legitimate interest for processing, in which case Steinweg will communicate such legitimate interest in advance.

If none of the above are satisfied then Steinweg will make sure it has the necessary consent from the data subjects for the processing of their personal data. Steinweg will furthermore ensure that the consent conforms to the legal requirements of being specifically and freely given and in an informed and unambiguous manner.

It is important to note that a data subject has the right to withdraw its consent at any time and it must be easy for data subject to withdraw consent, as it was to provide it in the first place. It is important that there are appropriate processes in place to promptly action any withdrawal of consent.

Sensitive Personal Data
In some circumstances, Steinweg may also be required to process sensitive personal data. This could entail data relating to health, criminal convictions or offences, ethnicity, race or member of a union.

Processing sensitive personal data is subject to stricter controls and circumstances in which it can be processed than non-sensitive personal data. The legal grounds for processing sensitive personal data include:

- Where the processing is necessary for the purposes of carrying out obligations and exercising the specific rights of Steinweg for employment and social security and social protections law purposes;

- For the purposes of preventive or occupational medicine, the assessment of the working capacity of an employee;

- For equal opportunity purposes on the basis of substantial public interest, necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of difference racial or ethnic origins with a view to enabling such equality to be promoted or maintained;

- Where the processing is necessary for the purpose of, or in connection with, any legal proceedings, obtaining legal advice, or establishing, exercising or defending legal rights; or

- Where the data subject has given its explicit consent, to the extent permitted by law.

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of the official authority or when the processing is authorized by Union or Country Law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

B. Purpose limitation

Steinweg shall only collect personal data for clearly specified and legitimate purpose(s) and personal data must be handled in a way that is compatible with the original purpose for which data was collected. Personal data cannot be collected for one reason and then just be use for another. Any further purposes must be compatible with the original reason for collecting the personal data or legitimate in and of itself.

C. Data minimization

Steinweg may only collect and process personal data to the extent that is actually necessary for a particular purpose. In other words, it must not be collect personal data on a “nice-to-have” basis.

D. Accuracy

Steinweg shall take all reasonable steps to ensure that any personal data in its possession is kept accurate and up-to-date for the purposes for which it is processed. In addition, any inaccurate or outdated personal data shall be deleted or corrected without undue delay.

E. Storage limitation
Steinweg shall not keep personal data for longer than is needed for its intended purpose(s). This entails that the entities must have knowledge of its processing activities, established retention periods and periodic review processes. Steinweg Data Retention Policy establishes the guidelines for this purpose.

F. Integrity and confidentiality
Steinweg must ensure that appropriate security and technical measures are applied to persona data to safeguard it against unauthorized or unlawful processing as well as accidental loss, destruction or damage. The obligation also entails that the entities process personal data in a manner that ensures proper confidentiality.

Consequently and insofar as this is economically viable, personal data shall be anonymized or pseudonymised by the Company at an early stage during the processing and use thereof. Similarly, data shall be transmitted in an anonymized or pseudonymised form as far as possible, if reference to individuals is not required in order to achieve he purpose of the transmission.

G. Accountability
Steinweg is responsible for and shall demonstrate compliance with this Policy. Taking accountability requires a pro-active approach to privacy and data protection. Because of Steinweg taking accountability, it has implemented a number of measures, which include, but are not limited to:

- Ensuring that data subjects are able to exercise their rights applicable under data protection laws as described in Section 7

- Ensuring that the Company will have in place and maintain a number of data records to establish a maximum grip of personal data being processed.

  o Steinweg maintains de record of processing activities which include the following elements:
    - The activity;
    - The grounds for processing the personal data;
    - Who has access;
    - Whether the data is transferred outside the European economic area;
    - The retention period.

The record of processing activities should be a reference point according to which Steinweg can determine how personal data is being processed and why. It will be particularly useful when responding to queries as to how he persona data of data subjects is being processed. It is the responsibility of all departments to ensure that the record of processing activities is kept up to dat.

o Steinweg also has a record of consents to evidence that it was authorized to carry out the processing of a data subject's personal data where such processing occurred based on consent.

o Furthermore, Steinweg has in place and maintains a record of data incidents and data breaches. Steinweg is committed to combatting data vulnerabilities.

- Ensuring that third party data processors are also acting in accordance with this Policy.

5 Employee Fair Use Policy

This Employee Fair Use Policy is included in the general Data Protection Policy package. However, it must also be read and understood as an obligation of the employees in the performance of tasks at Steinweg insofar as those tasks involve the collection and processing of personal data.

1. Purpose and Content

1.1 In the role of employer, Steinweg needs to collect and further process personal data of its employees. Steinweg values your privacy and commits to protect your personal data. Steinweg's processing of personal data is conducted in accordance with the applicable laws, including but not limited to the European General Data Protection Regulation and the national GDPR implementation laws that aim to protect individuals privacy in connection with processing of personal data.

1.2 The purpose of this document is to provide information regarding how Steinweg collects, processes and shares personal data relating to employees. This document also provides information about the employees' rights in relation to the processing of their personal data.

2. What personal data will be processed?

2.1 Steinweg processes the following types of personal data about you:

- Contact information (e.g. name, address, email and telephone number);
- Personal identification numbers pursuant to legal obligations;
- Information about family members relevant for tax and insurance purposes (e.g. name and personal identity number);
- Information concerning the employment (e.g. information about the date of employment, position, salary, benefits, access and log information, information relating to performance and education);
- Material from camera surveillance (e.g. material collected in connection with monitoring of the worksite as described in article 8 of this policy);
- Financial information for payment purposes (e.g. bank and account details);
- Information about health (e.g. information about potential rehabilitation matters and absence);
- Communication (e.g. possibly stored information concerning data and telephone traffic and information regarding entrances and exits pursuant to article 8 of this policy).

2.2 As a general rule, Steinweg collects personal data directly from you. However, from time to time Steinweg may utilize the services of third parties to collect personal data about you, e.g. through publicly accessible sources and registers, such as public agencies or authorities.

3. For what purposes is personal data being processed?

3.1 Steinweg processes your personal data for the following purposes:

I To comply with applicable laws and regulations;

II For administration of the employment and to fulfill the employment agreement (e.g. to administrate salaries and benefits) and other related agreements;

III To handle health and security concern and to establish a contact point in the event of an emergency (e.g. an emergency contact person or family member);

IV To process employee work related claims (e.g. compensation, insurance claims, etc.);

V To follow up and apply to internal policies of the company;

VI To keep internal records updated with correct information;

VII To conduct performance reviews and employee surveys; and

VIII To give access and administrate access to IT-systems and other systems.

4. What are the legal grounds for processing of personal data?

Steinweg processes your personal data based on the following legal grounds:

I To fulfil our duties as an employer under applicable law;

II To perform our obligations in relation to the employment agreement;

III To protect vital interests of yourself or another natural person;

IV When we, as your employer, have a legitimate interest to process your personal data (e.g. for performance measures and employee surveys as well as for handling emergency contacts), except where such interest is overridden by your interests or the protection of your fundamental rights and freedoms s data subject;

V You have given consent to the processing of your personal data for one or more specific purposes.

5. How do we protect the personal data and when we do share your personal data?

5.1 Steinweg has taken the appropriate technical and organizational security measures to protect the personal data from loss, abuse and unauthorized access.

5.2 The number of employees at Steinweg that have access to the personal data is limited. Access to the personal data has only been granted the individuals at Steinweg that need to process the personal data in accordance with the purposes stated above. If necessary, Steinweg may transfer data within Steinweg group companies.

5.3 Steinweg may also share your personal data with third party suppliers providing services to Steinweg, e.g. suppliers or business partners that process personal data for the purposes of administrating salaries, IT systems and occupational health, etc.

5.4 Transfer of personal data to certain authorities or similar institutions may be conducted to the extent that it is necessary for administrating and fulfilling the employment agreement or because it is required by law or collective agreements.

5.5 Sometimes it may be required to transfer personal data concerning employees to third countries, e.g. from countries within the EU/EEA to countries outside the EU/EEA. In such event Steinweg will make sure transfers only take place to countries which have an adequate level of data protection or which have appropriate safeguards in place.

6 How long is your personal data retained?

6.1 Steinweg applies different retention periods for different categories of your personal data. There is a Data Retention Policy for this purpose.

6.2 In general, the personal data will be retained during the employment period. After the employment period it will be retained as long as there is a legitimate purpose and the retention is in accordance with applicable law. When the processing of the personal data is no longer necessary for the purpose for which it was collected Steinweg will erase the personal data.

7. What are your rights and remedies?

7.1 Right to be informed

You have right to request information on how your personal data is processed and what personal data is processed about you.

7.2 Right of access

You have the right to receive a copy of the personal data that is being processed and held by us.

7.3 Right of correction

If you discover that the data we hold about you is incorrect or incomplete, you have the right to have the data corrected.

7.4 Right of erasure

You have the right to request data deletion. We are required to delete the data we hold on you in the following circumstances:

a) Where it is no longer necessary for us to keep the data;
b) Where we relied on your consent to process data and you subsequently withdraw that consent (and in absence of another legal basis for our continued use of your data);
c) Where you object to the processing and we have no overriding legitimate interest to continue processing.
d) Where we have unlawfully processed your data;
e) Where we are required by law to erase the data.

7.5 Right of restriction

You have the right to require restriction of the processing of your data in the following circumstances:

a)Where you tell us that the data we hold on you is not accurate or we do not have a legitimate interest to process such data: until such time that we have taken steps to ensure that the data is accurate or determined it is appropriate to continue to process the data;
b)Where the data has been processed unlawfully;
c)Where we no longer need to process, the data but you need the data in relation to a legal claim.

Where data processing is restricted, we will continue to hold the data but will not process it unless you consent to the processing or processing is required in relation to a legal claim.

7.6 right to withdraw consent

If you have given your consent to processing of your personal data for an explicit purpose you may always withdraw your consent. If you want to withdraw your consent, you may contact Steinweg though the contact information provided in Section 9.

7.7 Right to data portability

To the extent Steinweg processes your personal data based on consent or the necessity to fulfil a contract and the processing is carried out by automated means, you have the right to, upon request, to receive your processed personal data in a structured, commonly used and machine-readable format and the right to transmit your personal data to another controller.

7.8 Right to object

It is important for Steinweg that you feel safe in relation to Steinweg's processing of your personal data. Steinweg values the integrity of all employees and aims to process all personal data with respect. If you nevertheless think that your personal data is processed wrongly please do not hesitate to contact us. You are also entitled to lodge a complaint to the supervisory authority.

8 Privacy on the work floor; monitoring

8.1 Steinweg makes various communication resources available to its employees, such as email and Internet access. Use of these means of communication often results in the processing of personal data. Steinweg typically needs to process data in order to carry out its contractual obligations with its employees. Steinweg takes the processing of personal data of its employees very seriously and its committed to maintaining the highest data protection and data security standards.

Besides carrying out employment obligations, Steinweg may have legitimate interests to process other personal data while safeguarding the interests of its employees and contractors as much as possible.

8.2 Steinweg as an employer is committed to respecting the privacy of its employees and contractors. In practice this means that:

- The company does nog engage in any active monitoring of email and Internet use. This pertains to both business and private email and Internet use;
- Employees may use the email and Internet facilities for private use during office hours and at the Company premises, provided that:

o Such use does not interfere with the duties of the employee. The work may not suffer because of this use;
o The use of email and Internet does not violate Steinweg's Code of Conduct. All behavior should follow rules of common sense and decency and of etiquette.

8.3 Some exceptions do exist. While Steinweg has a lenient email and Internet Policy for private use, the Company is also committed to ensuring that effective data security safeguards are in place. Our IT department is occupied with the prevention and handling of external cyber threats on a day to day basis. Business continuity and disaster recovery are the #1 challenges for our IT department.

8.4 Please be advised that Steinweg does not monitor or investigate at random but will typically only do so in any of the following events:

- Steinweg has been alerted to the occurrence of a generic threat, such as a virus, a DDoS or ransomware, and Steinweg has reason to assume that it may be impacted;
- Steinweg has reason to assume that its economic, trade and financial interests may be at risk;
- Steinweg has been alerted that its IT systems or its physical systems may have been adversely impacted;
- Steinweg has been informed that confidential information, trade secrets or intellectual property rights may have been compromised;
- Steinweg has been informed that its Code of Conduct has been violated by any of its employees or contractors, which may include illegal, defamatory or abusive acts as further described therein.

Above list represents the main type of events, but may also be complemented by other events where the legitimate interests of Steinweg are involved.

8.5 In case monitoring is necessary Steinweg will keep any interference of the rights of our employees at a minimum.

8.6 This policy is also applicable to contractors of Steinweg. Steinweg reserves the right to update this policy from time to time and will request the employees to re-read the policy after such update. We expect your support in making the Company a good and safe place to work.

9. Contact information

Each local Steinweg entity is the data controller for the processing of personal data in that country/legal entity. This means that each local Steinweg entity is responsible to ensure that the personal data under its supervision is being processed in a correct manner and in accordance with applicable legislation. The Global Compliance Manager may be contacted for data protection matters in relation to Steinweg Global issues. For compliance with the European GDPR Steinweg chooses domicile in the Netherlands and submits to the jurisdiction of the Dutch privacy law authorities (“Autoriteit Persoongegevens”)

Data subjects can contact the Global Compliance Manager (Compliance@nl.steinweg.com) or their local managements in order to exercise their rights. If an Employee or director of the Company receives such message from a data subject, they should inform the Global Compliance Manager thereof.

5 Data Transfer Policy

Specific legal requirements apply to the transfer of personal data out of the European Economic Area ("EEA"). The transfer of data includes sending data to another country or allowing that data to be accessed remotely in another country.

Personal data must not be transferred outside the EEA unless an adequate level of protection and/ or appropriate safeguards for the rights and freedoms of data subjects are ensured. This can be satisfied by:

i.The recipient country having been subject to an adequacy determination by the European Commission;

ii.The implementation of binding corporate rules;

iii.The entry into data transfer agreement between Steinweg and the non-EEA recipient of the personal data via standard contractual clauses that have been approved by the European Commission; or

iv.The Trans-Atlantic (EU-US) Data Privacy Framework

6 Third Party Service Providers

Services who process personal data as defined in the European GDPR under the instructions of Steinweg are subject to the obligations on processors in accordance with Article 28 of the GDPR, irrespective of where that service provider or the instructing Steinweg entity is located. As a consequence where Steinweg instructs a third party to process personal data on its behalf, Steinweg will enter into a written data processing agreement with this third party as required under the GDPR. Such data processing agreement will among other things require the third party data processor to process the personal data only in accordance with Steinweg's written instructions and also mandate the third party processor to implement appropriate technical and organizational measures and controls to ensure the confidentiality and security of the personal data.

When contracting with a third party data processor, it is important that Steinweg conducts appropriate due diligence both at the outset of the relationship and on a periodic basis. The due diligence should ensure that the third party data processor is capable of complying with the requirements of the written agreement as detailed above.

7 Breach Management

All issues and potential data protection breaches under the European GDPR should be reported to the CISO, Global Compliance Manager and the local management. All personnel must be aware of their own personal responsibility to escalate potential issues as well as suspected or actual data protection breaches, as soon as they identify them. As soon as an incident or actual breach is discovered, it is essential that escalation action within Steinweg are undertaken immediately since the GDPR requires breaches with a certain risk profile to be notified to the relevant data protection authority within 72 hours after discovery.

Potential breaches will also include any breaches of this Policy. For the avoidance of doubt any control weaknesses identified should also be escalated to the GRC Director. Security incidents will be immediately reported to the CISO to cybersecurity@steinweg.com.

Steinweg also expects any third party service providers to report any potential or actual data protection breaches as soon as they identify them to their contact within Steinweg. The Security Incident Team will ask you the details of the incident and will prepare a root cause analysis and coordinate corrective and preventive actions.

8 Team

IIt is the responsibility of the respective management of all legal entities within the Steinweg group to adopt, implement and ensure timely compliance with this Policy and all applicable data protection and privacy regulations, and to be able to demonstrate such compliance.

In addition each local Steinweg entity may be under legal obligation to implement local policies and routines as necessary to fulfil the legal requirements for data protection purposes and requirements.

Data protection is not a sole exercise. We have a whole team ready and able in the Company with certain defined roles.

Roles

- **Management** (in practical terms: the director(s) of the legal entity) is responsible for ensuring that the data protection management system (DPMS) is implemented and maintained in accordance with this policy and that all necessary recourse are made available.

- **Group Compliance Manager** is responsible for for this document. This Policy may be updated regularly and be communicated to Steinweg's Employees and partners. Also (S)he is responsible to handle request about subject's data request while enforcing their rights

- **CIO or IT manager** (or in his/her absence, management) is responsible for protecting the integrity, availability and confidentiality of IT systems and shall take suitable measures to achieve this. (S)he is the contact person for the Director of Compliance as regards all questions regarding technical and organizational measures.

- **CISO**. The role of a Chief Information Security Officer (CISO) is to ensure the security of an organization's technology and data. The CISO is responsible for developing strategic plans to handle the security and compliance of the organization's information assets and to protect against data loss, theft, or unauthorized use. He/she needs to work with colleagues in data protection, privacy protection, IT infrastructure, compliance, and software development to ensure compliance with data protection and privacy laws, standards, and guidelines.

- **Human Resources management** is involved in the coordination of organizational measures and serves as a point of contact for the Global Compliance Manager in this regard, It will verify the intended rules from an employment law perspective and if necessary coordinate these with the employees or their representative bodies.

- **All employees** must comply with the internal regulations, in particular the regulations regarding data protection and IT/information security.