Privacy Policy

We are pleased that you are visiting our website and thank you for your interest in our company and products, as well as the related information and services. For certain of our services you send us personal data. The security and confidentiality of your personal data during your use of our website and our services are very important to us.

This policy deals with the relevant principles of the protection of personal data and their implementation.

Definitions

“Anonymisation”: process by which personal data are converted so that they cannot be traced back to the data subject. Once this has taken place, the data are no longer deemed to be personal data.

“Employees”: directors, senior managers, managers and employees of CO.DON AG and its subsidiaries.

“Consent”: any freely given, specific, revocable and deliberate indication of agreement by an individual to the recording and processing of his or her personal data.

“Data security breach”: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

“Data processing by a processor”: means that a third party is engaged to process personal data, without assuming responsibility for the respective business process.

“Explicit consent”: a person is given a clear option to agree or not to the collection, use or disclosure of personal data and the person makes a clear indication of their choice.

“Person”: a natural person to whom the personal data belong.

"Personal data": all information related to a person and by means of which a person can be identified by someone else. The person can either be identified directly (e.g. by a photo or name) or indirectly (e.g. by a health insurance number). In some countries, personal data may also include information such as the serial numbers of medicine products, biological samples, IP addresses or information about a company (“legal person”).

“Data protection policy”: is an oral or written statement that is shown to a person when their personal data are collected. It defines from whom personal data are collected and for what reasons, how the data are used, disclosed and stored and all the other relevant information that the data subject should know. Any oral statements must be recorded to prove that the person has been informed and should be included in any local standard operating procedures.

“Process”: every procedure carried out with personal data. The definition also comprises collection, recording, organisation, storage, retrieval, use, disclosure, anonymisation, pseudonymisation and deletion.

"Pseudonymisation": the name of the person and most other identifying features are replaced by a label, a code or another identifier in order to protect the person from being identified. Pseudonymised data are still personal data.

"Sensitive personal data": are personal data which require greater protection. They include information about race, ethnic origin, political opinions, religious or philosophical convictions, trade union membership, social security or insurance information, criminal charges/convictions, sexual orientation and health. The definition of sensitive data may vary from one country to another. Local legislation must be followed.

"Third parties": is every natural or legal person with which CO.DON is in contact and in the case of legal persons, which is not a CO.DON company or an associate.

"Traceability": refers to the ability to trace information, in order to follow all additions and changes to personal data and the location of personal data. It helps CO.DON to demonstrate its transparency and compliance with regulations.

"Transfer": means any disclosure of personal information by someone other than the data subject. The term "transfer" may include the physical forwarding of personal data or the provision of access to personal data.

Principles and rules

Compliance with legislation

The Code of Conduct of CO.DON AG contains fundamental principles and rules for business ethics, including the acknowledgement of data protection rights and the obligation to protect the personal data of our employees and other individuals whose personal data are forwarded to CO.DON.

As employees we have a particular responsibility for meeting this obligation, as described in this policy and in the relevant data protection laws.

Employees must be aware of the general data protection provisions and principles applicable to personal data and know when to notify their manager of a problem. Employees are expected to recognise whether they collect, process, forward or use personal data.

Fair and lawful collection and use of personal data

The basic principle of data protection calls for the fair and lawful processing of personal data by CO.DON.

Employees should:

- Only collect and use personal information with a lawful justification, which may include CO.DON's legitimate commercial interests. For example, some local legislation may require the explicit consent of the data subject before personal data is collected (e.g. informed consent for clinical research).
- Notify the individuals of the use of their personal data before the data are collected.
- Only collect the personal data that are necessary for the particular commercial purpose.

- Only use personal information for the specific commercial purpose described in the data protection policy or the consent form, or in a way that the person would reasonably expect.
- Use personal data in a way that has no adverse effects on the data subject, unless such a use is justified by law.
- Anonymise or pseudonymise personal data when possible or appropriate.

Responsible administration and maintenance of personal data

All employees are responsible for complying with the data protection provisions concerning personal data. Employees who collect, use and/or administer personal data must take the appropriate steps:

- To keep personal data correct and up to date during its entire life cycle (i.e. from collection to erasure).
- To protect personal data so that it is not disclosed to third parties with no valid commercial reason for accessing the data.
- To prevent the misuse of personal data for a purpose which is inconsistent with the purpose for which they were originally collected.
- To ensure that personal data are traceable during their entire life cycle.
- Only to retain personal information for as long as necessary for the specific purpose or as long as required by law.
- To report a data protection breach to their supervisor, executive management or the legal department.

Information on the disclosure of personal data to third parties and other CO.DON partners

Personal data may be disclosed to other CO.DON employees, public authorities or other third parties to the extent permitted or required by legitimate commercial reasons or statutory provisions. The third party must confirm that they will protect the personal data in accordance with the standards and principles mentioned in this policy. Such confirmation may be obtained by a third-party due diligence, risk assessment and/or contract. A processing agreement is necessary if third parties are given access to personal information in order to process it on behalf of CO.DON AG. All agreements must include the data protection principles and processing notice. On the basis of third-party risk assessments, suitable technical precautions (e.g. encryption) or other measure must be contractually agreed to ensure the appropriate protection of personal data.

Data processing by a processor

An agreement must be signed between the external providers and CO.DON AG in all cases of data processing by a processor. The external provider only processes the personal data in accordance with the instructions of CO.DON AG. CO.DON AG is entirely responsible for the correct processing of the data. When engaging the processor, the employee concerned must ensure that the following conditions are met:

- The provider is selected on the basis of its ability to ensure the necessary technical and organisational measures for protecting data.
- The engagement must be in writing. The notice on data processing and responsibilities must be documented by CO.DON AG and the processor.
- Before data processing begins, CO.DON AG must be able to rely on the processor meeting its obligations. A processor can document that it meets the data protection requirements by means of a corresponding certification. Depending on the risks of data processing, the audits must be repeated at regular intervals over the course of the agreement.

Information on the cross-border transfer of personal data

In some cases the use of external processors may include the transfer of personal data across national borders. Insofar as personal data are transferred to processors across borders, the following steps are required:

- It must be determined whether a legitimate reason for the transfer of personal data exists.
- Information (e.g. valid commercial reason);
- The local SOPs must be followed for all other local statutory requirements (e.g. notification of the data subject, notification of data protection authority, use of contractual measures such as EU standard contractual clauses).

Right to access, rectification, revocation and objection

Information right

You have the right to information about the type of personal data, their origin and the purpose for which they are processed. Furthermore you have the right to information about the controller responsible for the processing of your personal data and if the personal data are transferred, about the recipient. To the extent that automated decisions are concerned, this information right also extends to the logical structure of the automated processing stages.

To the extent provided for by local law, the information right does not apply if it would cause a significant impairment of commercial intentions. This applies particularly if the disclosure and the interest in maintaining commercial secrets outweigh the individual's interests in disclosure. The information right may also be restricted by local regulations if the information right is exercised repeatedly within a short time and no legitimate reason for the repeated request is provided. To the extent permitted by applicable national law, CO.DON AG may charge a reasonable fee for providing the information.

Right to rectification

Every data subject has the right to require the rectification of personal data insofar as they are found to be incorrect or incomplete.

Right to blocking

You have the right for your personal data to be blocked if it is impossible to determine whether the data are correct or unimportant.

Right to erasure

You have the right to require the erasure of your personal data if the data processing was or became unlawful or when your data are no longer needed for the processing purpose.

Justified claims to erasure by a data subject must be made within a reasonable period, to the extent that statutory or contractual record-keeping obligations are no obstacle to the erasure.

In the case of statutory record-keeping obligations the data subject may require the personal data to be blocked and not erased. The same applies when it is not possible to erase the data.

Right to object

You have the right to object to the processing of your personal data for advertising purposes or for market research and/or opinion polls. Every data subject should be notified of the right to object without charge.

You also have the general right to object to the processing of your data to the extent that in view of the particular personal situation of the data subject, the legitimate interest of the data subject outweighs the legitimate interest of the controller in the processing of the personal data.

Procedure

Please send your request to datenschutz@codon.de. As far as possible, CO.DON AG will respond within four weeks to the request to access, correct, rectify or amend your personal data. If your request does not contain sufficient details for a response, CO.DON AG will ask you for additional information.

Employees of CO.DON AG are to consult the Legal Department before rejecting a request for access, rectification, erasure or an objection to the processing of personal data. If your request is rejected, CO.DON AG will send you an explanation.

Whistle-blowing

All employees are obliged to notify their supervisor, the Legal Department or the management without delay if they suspect a potential breach of applicable law and/or of this policy.

Employees who report or help to investigate potential breaches are protected against retaliation.

Breaches of this policy

Disciplinary and other measures, up to and including dismissal, may be taken in the event of a breach of this policy.

Responsibilities

Every employee of CO.DON AG with responsibility for staff is responsible for following this policy in their functional area, acting as a role model and instructing their staff on the policy.

All employees of CO.DON AG are obliged to comply with the policies and principles described here.