# DATA PROTECTION POLICY

## 1. Introduction

When doing business, Retta Group Oy and its subsidiaries ("Retta") collect, use and store personal information about its employees, customers, business partners and other individuals. Retta has a responsibility to ensure that it handles this information responsibly in order to protect individuals´ personal data.

Code of Conduct Policy is Retta´s top policy, which collects all other policies together. Different policies are described shortly in our Code of Conduct Police and made reference to each specific policy.

This Data Protection Policy is designed to help Retta to comply with the European General Data Protection Regulation (GDPR). Retta also ensures to comply with all applicable national legislation wherever it operates.

This Policy applies to all employees belonging to Retta group of companies ("Retta") and Boards of Directors of Retta companies.

This Policy applies to all companies and operating countries of Retta. This Policy and related guidelines and work practices are designed to ensure that also all employees are aware of and comply with their obligation to protect the privacy of all individuals and the security of such individual's Personal Data.

Retta has also internal instructions for its employees about data protection. In case of any discrepancies between this Policy and other instructions, this Policy prevails.

## 2. Data protection concepts

| | |
|---|---|
| *Controller* | When Retta processes personal data, it will usually do so on its own initiative, determining why and how the personal data will be processed, acting as "controller". |
| *Data subject* | A data subject is an individual whose personal data is being processed |
| *Joint controllers* | Sometimes two or more organizations might work together to decide why and how personal data is processed. This is referred to as "joint controllership" and should be governed by a joint controller agreement that determines the controllers' respective responsibilities. |
| *Personal data* | Personal data is information relating to an identified or identifiable individual, for example name, social security number, online screen name, location data, or an identifier such as their physical, physiological, genetic, mental, economic, cultural, or social identity |
| *Processing* | Processing is the handling of personal data, including collecting, using, adapting, transmitting, storing, and even erasing personal data. |

| | |
|---|---|
| *Processor* | "Processor" is the term given to companies processing personal data purely on behalf of, and under the instructions, of another company. Controller-processor relationships must be governed by a data processor agreement ("DPA"). |
| *Special categories of personal data* | Some categories of personal data are generally prohibited from processing, unless specific derogations apply. Such categories are sometimes referred to as 'sensitive data' and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. |

## 3. Data protection principles

Certain principles apply to every data processing activity. Retta must comply with each of the principles described below.

### Fairness and lawfulness

Retta must only process personal data on certain specific legal grounds, and must take into account any elevated risks to the privacy of data subjects.

### Data minimization and purpose limitation

Personal Data may only be collected for a specified, explicit and legitimate purposes that are compatible with the original reason for collecting the personal data, and only to the extent necessary for achieving that purpose. Retta's systems and procedures should be designed to uphold these principles.

### Accuracy

Retta must ensure that it takes active steps to ensure that the personal data it has on file is accurate and up-to-date.

### Integrity and confidentiality

Retta must implement appropriate technical and organizational measures to achieve an adequate level of security for its personal data processing activities. Retta must also ensure it maintains the integrity of its personal data processing activities, taking steps to prevent accidental data loss. In doing so, it will take into consideration relevant state-of-the-art technology; the costs of implementation; and the nature, scope, context, and purposes of the processing.

### Transparency

Company must ensure it is open and forthcoming with data subjects about what personal data of theirs it processes and how the processing is performed. Openness is put into practice in Retta, for example, by providing information about processing activities on the Retta's webpages. All data subjects shall be

offered information on what kind of Personal Data is being processed and how is the Personal Data being processed. Retta ensures that all data subjects are aware of how to exercise their rights as data subjects.

### Storage limitation

Retta must have a systematic approach to maintaining records in order to comply with applicable laws and regulations, to protect its interests, and for business continuity. Personal data, however, should not be stored for unnecessarily lengthy periods or without an overriding interest given the risk this poses to the privacy of individuals.

### Accountability

The accountability principle requires Retta to take responsibility for and demonstrate compliance with processing personal data in compliance with the principles described above. Retta must have appropriate measures and document such measures, e.g. adopting and implementing data protection policies, maintain documentation of data processing activities, carrying out data protection impact assessments, etc.

## 4. Legal basis for processing personal data

Retta can only process personal data if it identifies specific legal grounds permitting such processing. Retta should always be aware of which legal ground it is relying upon when carrying out a processing activity. More restrictive conditions apply to special categories of personal data, as explained below.

| | |
|---|---|
| *Legal obligation* | Retta may process personal data to the extent necessary to fulfil a legal obligation (e.g. KYC- obligation). |
| *Performance of a contract* | The data processing is necessary for Retta to fulfil its obligations in a contract that it has entered into with the data subject (e.g. retaining bank account details to pay a salary under an employment contract), or in order to take steps at the request of the data subject prior to entering into a contract. |
| *Legitimate interest of the Company* | Retta may process personal data for legitimate purposes as part of its business. (e.g. keeping a database of information on its customers or business partners, or collecting the names and phone numbers of emergency contacts of its employees). However, the legitimate interest must be specific, and justified when weighed up against the fundamental rights of the data subject, including their right to privacy. |
| *Consent* | The data subject has agreed to the processing. Consent must be freely given, specific, informed, and unambiguous. Data subjects must be informed that they can withdraw their consent at any time. |
| *Other* | Although they are rarely applicable, there might be other grounds on which personal data may be processed, namely the protection of the vital interests of the data subject or tasks carried out in the public interest. |

### 4.1 Legal basis for processing special categories of personal data

Certain special categories of personal data are afforded extra protection and should not be processed by a company except under specific circumstances. Such personal data is for example personal data that reveals racial or ethnic origin, reveals political opinions; reveals religious or philosophical beliefs; reveals trade union membership; concerns an individual's health; concerns an individual's sex life or sexual orientation; and certain forms of biometric data.

If special categories of personal data is processed for any reason, higher levels of data protection are necessary and in some cases, data protection impact assessments must be conducted.

### 4.2 Direct marketing

When carrying out direct marketing Retta must ensure that there is a legal ground for the processing of personal data, that data subjects receive sufficient information about the processing, and that data subjects are able to exercise certain rights such as the right to object/opt-out, right to access, right to rectification, erasure, and restriction.

## 5. Data subject´s rights and information to data subjects

The GDPR gives data subjects a number of rights as regards the processing of their personal data. Retta must observe those rights and ensure that adequate procedures are in place to accommodate data subjects.

Enquiries by data subjects to exercise their rights must be dealt with swiftly and Retta must act on an enquiry within one month after it was received. In certain cases longer time may be necessary and justified. Retta is under a duty to take all reasonable actions to check the identity of the data subject.

An enquiry received by any employee of Retta should always be immediately forwarded to Retta´s Data Privacy Coordinator or Local Privacy Coordinator for further action, according to Retta´s internal instructions.

| | |
|---|---|
| *Right to information* | Data subjects have the right to information when the personal data are collected. Retta has published internal privacy notices in Company´s intranet, with information on how it processes employee personal data. Third parties are informed via privacy notices available in Company web page. |
| *Right of access* | Data subjects have the right to receive a confirmation of whether or not their personal data are being processed by Retta and, if so, gain access to their personal data by receiving a copy of the personal data that are processed (often referred to as a data subject access request). |
| *Right to rectification, erasure ('right to be forgotten')* | Data subjects have the right to have inaccurate or incomplete personal data concerning them rectified or supplemented without undue delay. In some cases data subjects have the right to request erasure of their personal data ('right to be forgotten'). Examples of this are when consent is the legal basis for the processing and the data subject withdraws their consent or if the data subject demonstrates |

| | |
|---|---|
| *and restriction* | that the data are no longer necessary for the purposes for which they were collected.<br><br>In certain circumstances data subjects can demand that the processing of their personal data be restricted. This means that Retta may only store the personal data and not process them further without the data subject's consent. The right to restriction applies, among other things, when the data subject considers that the data are inaccurate, and has requested they be rectified. The data subject can then request that the processing of the personal data be restricted while their accuracy is ascertained. The individual must be informed when the restriction ends. |
| *Right to object* | Data subjects have the right to object to Retta's processing of personal data when the processing is based on Retta's legitimate interest. When a data subject objects, Retta must cease processing unless it can demonstrate legitimate grounds that outweigh the rights of the data subject. When personal data are processed for direct marketing purposes, data subjects have the right to object at any time to processing of their personal data. If a data subject opposes processing of personal data for direct marketing purposes, processing for such purposes must cease. |
| *Right to data portability* | Data subjects have the right to transmit personal data they have provided to Retta to another controller (the right to data portability) if the processing is based on contract or consent, and is carried out by automated means. The personal data must be provided to the data subject in a structured, commonly used and machine-readable format. If it is technically feasible, the data subject can request that the data be transmitted directly to another controller. The right applies solely to personal data that the data subject has provided to Retta. |

There are some exceptions where Retta is not obliged to accommodate a request as described above for example if such a request would conflict with Retta's legal obligations.

## 6. Record of processing activities

In accordance with GDPR, Retta maintains a record of all processing of personal data carried out at Retta. The record must contain certain information, such as a description of the categories of personal data and the legal basis for, and purpose of, the processing. On request, the record must be submitted to the relevant data protection authority or other relevant data protection authorities.

## 7. Data breach procedure

A personal data breach is a security incident that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that Retta transmits, stores or otherwise processes (e.g. as a result of hacking, a integrity sensitive email to the wrong recipient or an error in a system that causes data to be lost). If a personal data breach occurs that may result in a risk to the rights and freedoms of private individuals, Retta must report this to the relevant data protection authority or the relevant data protection authority as required by applicable legislation no later than 72 hours after the breach is discovered, and in some cases also inform data subjects. When the personal data breach is

likely to result in a high risk to individuals, Retta shall also communicate the data breach to the individuals without undue delay.

Please note that Retta may also need to notify other third parties of a data breach, such as insurance companies and relevant parties in accordance with contractual obligations. Retta has internal instructions for data breach process.

## 8. Use of data processors and international data transfers

Whenever Retta enters into a relationship with a third party involving the exchange or transfer of personal data, Retta must enter into a written agreement with the third party. This helps to ensure that whoever is processing the personal data does so in a legally compliant and responsible manner.

Whenever Retta exchanges or transfers personal data to a third party that will have the role of a processor, this must be subject to a data processor agreement containing certain requirements. The processor may only process personal data on behalf of Retta according to the instructions laid out in the processor agreement.

Retta has model templates for Data Processor Agreements, which Retta employees are guided to use whenever possible.

When applicable: Retta must ensure adequate protection measures when transferring personal data outside of the EU/EEA. This can be done through one of the following routes:

| | |
|---|---|
| ***Option 1***<br>*Transfers on the basis of an adequacy decision* | Personal data can be transferred outside of the EU/EEA if the country or entity to which it is being transferred is deemed to have adequate protection by the EU Commission. |
| ***Option 2***<br>*Appropriate safeguards* | If Option 1 is not available, Retta should sign an agreement with the non-EU/EEA party using the EU Standard Contractual Clauses for international transfers (the "**SCC**"). Prior to entering into the SCC, Retta must examine the circumstances surrounding the transfer to a non-EU/EEA recipient, as well as assessing the adequacy of personal data protection in the importing country and document the assessment in a transfer impact assessment ("**TIA**"). If the TIA reveals that the importing non-EU/EEA country is deemed to have an inadequate protection for personal data supplementary measures (legal, technical or organizational) must be put in place (in addition to SCC). |
| ***Option 3***<br>*Specific derogations* | If Options 1 or 2 are not used, personal data can be transferred outside of the EU/EEA if a special legal exception (or "derogation" as it is called) applies. Examples of such specific derogations are:<br><br>(a) explicit consent from the data subject after having been informed of the possible risk of such transfer due to the absence of an adequacy decision or appropriate safeguards;<br><br>(b) the transfer is necessary for the performance of a contract between the data subject and the controller or |

the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the establishment, exercise or defence of legal claims.

## 9. Privacy by design and privacy by default

Retta must ensure compliance with applicable data protection legislation (including GDPR) each time personal data are processed. This means that when IT systems and procedures are formulated Retta must take appropriate technical and organizational measures to meet the requirements of GDPR and protect the rights of the data subject ("privacy by design"). Retta must also ensure that, in standard cases, personal data are not processed unnecessarily, and are not made available to an unlimited number of private individuals (privacy by default).

## 10. Data protection impact assessments

Even if there is a valid legal ground to process personal data, Retta must first conduct a data protection impact assessment (DPIA) if it wishes to engage in data processing activities that are likely to result in high risks to the rights of freedoms of individuals (e.g. installing camera surveillance in office areas). A data protection impact assessment is a process to help identify and minimize the data protection risks of a processing activity. Please contact Retta´s Data Privacy Coordinator for more information and/or instructions.

## 11. Personal data on social media platforms

Whenever Retta has accounts on social media platforms (e.g. Facebook, Instagram, Twitter, YouTube, etc.) for communication and marketing, it acts as controller for processing of personal data on its own accounts to the extent that Retta is in control of such publications and has the possibility of making adjustments/delete such information.

Whenever Retta uses tools provided by a social media platform, e.g. marketing or analytics tools, there might be a joint controllership between Retta and the social media platform.

To the extent that Retta is controller, it is required to ensure that its processing activities comply with the content in this manual.

## 12. Use of cookies on websites and apps

Retta, as a website or app owner, is responsible for providing users with appropriate information and collecting consent before using cookies to collect, store or process personal data.

Whenever Retta uses cookies on its websites or apps, it must have and provide a cookie policy. The cookie policy must be available on the website or app and must contain information to the user of the purposes for which cookies are used (e.g. marketing, statistic or functional cookies), how the information collected about the user is processed and if the information is shared with any third parties.

In addition to a cookie policy, websites and apps must have a banner or pop-up form that informs users of Retta's cookie policy and asks users to consent (or reject) to the use of cookies. The consent must be specific for each purpose, and the user must consent to each specific use.

## 13. Data Protection Organization

Retta has data privacy organization with named responsible persons. At the Group level, the Data Privacy Coordinator leads and is responsible for Retta´s data privacy. A designated GDPR core team supports Data Privacy Coordinator in her/his role. The Data Privacy Coordinator has independent position and a straight communication channel to Retta´s Board of Directors. Locally, Retta has local privacy teams and Local Data Privacy Coordinator in all countries where Retta operates. Local organizations are responsible for assessing and complying with local regulations regarding the processing of Personal Data. Local Data Privacy Coordinator reports to Data Privacy Coordinator and is part of GDPR core team. Every employee, manager and Board of Directors of Retta companies must be familiar with this Policy as well as the relevant guidelines given based on this Policy.

Any activity that is in breach of (i) this Policy, (ii) internal guidelines or instructions given based on this Policy or (iii) data protection legislation, is considered to be a data protection incident. All incidents must be reported as described below in Section 15 and investigated appropriately.

## 14. Commitment

Each employee, manager, executive officer and member of the Board of Directors must understand and comply with this Data Protection Policy. Managers should ensure that their teams fully understand and are expected to comply with the standards and requirements stipulated in this Data Protection Policy.

If you have any questions about the content of this Data Protection Policy, or how it should influence your everyday work or a specific matter, please reach out to Retta´s Data Privacy coordinator or Local Data Privacy Coordinator.

## 15. Training

Retta provides general trainings to its Board members, management and employees on data protection compliance. Trainings are repeated at regularly.

## 16. Reporting concerns and consequences of violation

If you become aware of or suspect a possible violation of law, rule or regulation you are required to promptly contact Retta´s Head of Legal.

If you become aware of violation of this Policy or any other of Retta’s policies, you shall contact Retta´s Chief Compliance Officer, CEO, Head of business unit or your closest supervisor.

You can also raise concerns through Retta’s whistleblowing system available in Retta´s web pages. Retta will not tolerate any attempt to take adverse action against an employee for reporting a genuine concern regarding suspected wrongdoings. Retaliation against anyone who speaks up is a violation of the Code of Conduct and will not be tolerated.

Retta does not tolerate any illegal or unethical behavior. Violations of this Policy is likely to damage Retta’s brand and reputation. Failure to follow this Policy is taken seriously and may result in disciplinary action appropriate to the violation, including, but not limited to, termination of the employment.

## 17. Review and follow-up

Compliance with this Data Protection Policy by all Retta entities and employees will be monitored through internal and external audits, and routine follow-ups of all reported matters.

| Effective date | Version | Change description |
|---|---|---|
| 25.5.2018 | v1 | original |
| 20 December 2023 | v2 | updated |