Evac Data Protection Policy

1. Introduction

Evac Group Oy and its group companies (including shareholder companies up to Evac Holding Oy) (“Evac” or “Group”) collect, store, transfer, erase and otherwise process (“process”) various types of information concerning its employees, business contacts, customers and other individuals (“individuals”) for the purpose of carrying out Evac’s business operations.

Any data that relates either directly (e.g. name, email address or personal ID) or indirectly (e.g. customer ID, IP address or a device identifier) to these individuals, or which can be used to distinguish an individual, is considered personal data. Any processing of such personal data is governed by the relevant data protection and privacy laws.

This data protection policy (“Policy”) sets forth the main principles to be applied in all Evac’ personal data processing activities.

All Evac employees are expected to comply with this Policy. Employees who are suspected of having breached this Policy will be investigated. Any breach of this Policy will be considered and dealt with according to the applicable local laws and Evac’s policies and practices. This Policy does not limit the rights or responsibilities of Evac or its employees to act according to local laws when applicable and necessary.

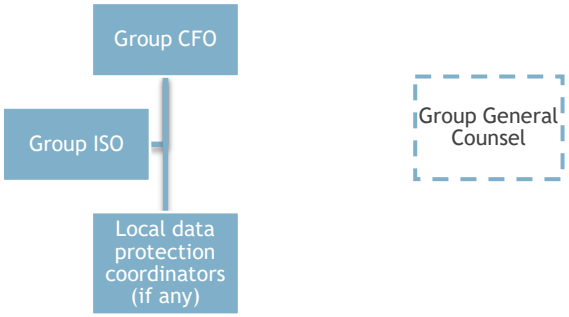
In addition to the requirements set forth in this Policy, applicable local legislation and contractual commitments need to be considered and complied with.

2. Purpose

Evac recognizes that personal data is a valuable and necessary asset for Evac’ success. The purpose of this Policy is to set consistent Evac standards to ensure that:

- privacy of individuals’ personal data is respected in all Evac operations;
- individuals feel confident that Evac respects and safeguards their personal data; and
- legal and regulatory risks, as well as reputational and brand exposure, with regards to Evac’ personal data processing activities are mitigated to an appropriate level.

3. Organization and governance of data protection



Group CFO has the overall coordinating role for all data protection matters within the Group. For cyber and information security matters, the Group has a dedicated Information Security Officer ("ISO") within the Group ICT team. Group may also have local data protection coordinators/contacts. Group General Counsel supports the data protection organisation.

The Company has not appointed a designated data protection officer as defined in the GDPR[1].

Data protection matters are regularly discussed among Group CFO, Group ISO and Group General Counsel. Group CFO reports material data protection matters to Group Leadership Team ("GLT"). GLT escalates matters to the Board of Directors of Evac Holding Oy where needed. Data protection matters are escalated on an annual basis to the Board of Directors in connection with legal and/or commercial updates.

Evac's business lines and relevant functions have the overall liability to maintain and monitor data protection compliance in their own businesses, with the support from the data protection organisation described above. Through training, all Evac employees and other authorized processors of Evac's personal data shall have appropriate expertise and awareness of requirements relating to processing of personal data in connection with their work duties.

Data protection shall be governed and managed according to Evac's governance model, which shall drive risk based continuous improvement on data protection issues.

4. Data protection principles

General data protection principles form the foundation of personal data processing within Evac. Whenever the business functions within Evac's organization are collecting and processing personal data, it is their responsibility to ensure that these principles are fulfilled, with the support from the data protection organization described in Section 3.

Any identified risks relating to non-compliance with these principles must be evaluated, reported and mitigated to an appropriate level within the relevant operational function prior to initiating the processing at question.

Lawful, fair and transparent processing

When you collect individuals' personal data, you must:

- Consider why is the data collected – if there is no clear and justified business reason for processing the personal data, it shall not be collected.

  Example: *Collection of employee data is necessary for the management of Evac's (employer) and employees' rights and responsibilities in relation to the employment relationship. There is, therefore, a concrete reason and need for the collection of employees' personal data. As a result, the collection of employee data is justifiable.*

- Transparency - ensure that individuals are aware about how their personal data will be used.

  Example: *Evac's privacy policies provide information to individuals and shall include all relevant information concerning Evac's personal data processing activities and therefore facilitate transparency.*

- Ensure the existence of appropriate legal grounds for the processing of personal data, such as individuals' valid consent, contractual necessity or Evac's legitimate interest.

  Example: *If fulfilling contractual duties require processing of personal data, the contractual relationship acts as the legal ground for the processing that is necessary for the fulfillment of that contract.*

- Seek advice from data protection organization, if you are uncertain of the legitimacy of the personal data processing.

[1] GDPR refers to the EU General Data Protection Regulation.

Purpose Limitation

When you process personal data, you must:

- Have a specified business purpose about why you need to obtain personal data.

  Example: *Personal data cannot be collected "just in case" or for purposes to be defined in the future. Defining the purpose must precede the actual data collection.*

- You may not use the collected personal data for purposes, which are not compatible with the initial purpose.

  Example: *Disclosing a list of Evac's employees' home addresses or family details to a third party for their direct marketing activities would not be compatible with the original purpose for which the employee has provided the information to Evac, and thereby such disclosure is not allowed.*

  Example: *If personal data is to be used for purposes that fall outside the original purpose, this is allowed only if such processing may be considered to be reasonably expected by the individuals concerned or after receiving consent of the respective individuals.*

Data Minimization

You need to ensure that:

- Personal data that you collect and record or hold is sufficient but not excessive for the defined processing purpose. To assess whether you are holding the right amount of personal data, you must first be clear about *why* you are holding and using it.

  Example: *When it is possible to meet the business targets and needs with aggregated, anonymous data, such data needs to be used instead of personal data. For example, business analytics not always require data on the level of specific individuals.*

  Example: *Information concerning employee's family relations (e.g. marital status, children's information, etc.) should not be collected, if there is no real reason for obtaining such data from the point of view of Evac's rights and responsibilities as an employer*.

- Local legal requirements for processing of national identification numbers and possible other similar personal data types, which are often regulated separately, shall be identified and such data processed only when necessary for the legitimate purposes defined and in compliance with the applicable law.

  Example: *Collecting individual's national identification number might only be allowed, when there is a specific legitimate reason and a legal basis for such collection (e.g. need for unique identification of the individual).*

  Example: *Collecting creditworthiness or criminal sanctions related data from job applicants or employees might be restricted under local law.*

Evac shall not process sensitive information about the individual, for example related to health, race, ethnic or social origin, religion or belief, political or any other opinion or property or disability concerning the individual.

The collection and processing of personal data of children is limited to what is considered appropriate and compliant in the given circumstances.

Data Accuracy

If you collect or use personal data, you need to:

- Take reasonable steps to ensure that the information is correct and valid. Reasonable steps may differ depending on the circumstances. If you will be using the data for reasons, which might be of significance for the individual, you need to put more effort into ensuring the accuracy.

- Consider whether it is necessary to update the information before you use the personal data.

Storage Limitation

When you collect or use personal data, you will need to:

- Consider the purpose for which you hold the data and not retain data for any longer than necessary for that purpose.

  Example: *Job applications shall not be retained for longer than necessary for filling the specific position (unless the applicant has consented otherwise), because the purpose of the data collection is a one-time recruitment.*

- Consider, whether Evac has a legal duty to retain certain data for a specified time period. If uncertain about that, seek advice.

  Example: *There are different legal retention periods that Evac must comply with. Such requirements may relate to bookkeeping (e.g. financial data) and employment (e.g. job certificates).*

- Securely delete or anonymize personal data, which is no longer needed for Evac's specific business purposes or for fulfilling legal retention obligations.

Privacy by Design

It is particularly important to ensure that the abovementioned principles are followed from the very beginning (privacy by design), when new processes, ICT applications, etc., which include processing of personal data, are implemented.

Example: *Evac sources services or materials from its suppliers. Prior to engaging into any contract with any such a supplier, sourcing function must consider whether a data processing agreement (DPA) is required.*

Example: *Evac is procuring a new CRM application, which will be hosted by a third-party vendor. Because the CRM system will hold some personal data of Evac's customers and potential clients, all privacy related requirements need to be considered from the very beginning to ensure that, for example, all necessary technical requirements are built into the system and necessary contractual measures are in place in due time.*

Example: *Evac is launching a new marketing campaign, where emails will be used as contact information. Because an email address, as a data attribute, is considered as personal data, the marketing campaign needs to be assessed from a data protection perspective prior to its launch.*

Example: *Evac has an HR system, which enables Evac to collect comprehensive information about its employees. Because the data processing relates to personal data of Evac employees, the legitimacy of the planned data collection (i.e. what data is allowed to be requested from the employee) needs to be assessed.*

Accountability

When you are planning personal data processing activities or are already processing personal data, you need to document everything that might be relevant for Evac to demonstrate accountability with regards to its data processing activities.

Data Security

Confidentiality

There shall be processes, procedures and appropriate non-disclosure agreement in place to ensure that employees and other authorized processors of Evac's personal data respect the duty of confidence and process personal data only when and to the extent necessary to perform their working duties. See also Group Confidentiality Policy.

> ***Example:*** *All employment and vendor agreements need to have appropriate confidentiality clauses.*

Appropriate Security Measures

Appropriate technical and organizational measures shall be implemented to protect confidentiality, integrity and availability of personal data in accordance with Evac' information and ICT security policies. These measures shall cover the whole lifecycle of personal data and ensure a level of security appropriate to the risks represented by the processing and nature of personal data taking into account the state of the art and the implementation costs of the measures.

> ***Example:*** *If a file containing personal data needs to be shared within or outside Evac, sharing it through a OneDrive link to specific people is a more secure alternative to email attachments.*

> ***Example:*** *If personal data must be stored outside Evac's HR system or other systems meant specifically for personal data, you must ensure that the location (e.g. Microsoft Teams channel) is only accessible to those who have a justified need to see the personal data.*

Data Breaches

Any unauthorized access, disclosure or erasure of personal data is considered a breach. You must report any personal data breaches or other comparable incidents immediately to Group ISO.

> ***Example:*** *If you accidently disclose personal data to a non-authorized party, that is considered as a personal data breach and shall immediately be notified to Group CFO, Group ISO or Group General Counsel.*

> ***Example:*** *If you suspect that somebody has used your personal or other person's passwords to access Evac's applications or data sources, you must immediately notify the Group CFO, Group ISO or Group General Counsel.*

5. Data disclosures and transfers

Disclosure to authorities

To ensure safety and confidentiality of Evac's personal data and compliance with legal and contractual requirements, personal data shall be disclosed to competent authorities (e.g. police) only to the extent required by law.

Transfer to external parties

Evac is responsible of the personal data also when personal data is transferred and processed by external parties ("data processors") on behalf of Evac.

- Before making any decision to transfer personal data to a data processor (e.g. service provider), possible risks and impacts of the transfer have to be assessed in order to make well-advised business decision, mitigate risks of the transfer and set appropriate requirements for the vendor regarding processing of personal data and safeguarding such processing.

- Prior to transferring any personal data to a data processor, necessary contractual measures need to be in place. Data processing agreement templates provided by Evac Group Legal function shall be used when possible.

  Example: *Personal data of an employee is sent to a service provider, which provides salary payment services for Evac. In conjunction with agreeing on other service terms, necessary contractual measures need to be taken in order to guarantee that data is managed and processed appropriately by the outsourcing (external) partner.*

  Example: *When personal data processing is centralized to Evac group headquarters (e.g. CRM application), it is seen as an outsourcing relationship between Evac group and the country organization, if the ownership of the data remains local. In such a scenario, an intra-group data processing agreement must be established (such agreement is in place at Evac).*

- Legal basis for personal data transfer from EU/EEA to a processor located outside EU/EEA needs to be established prior to the transfer. Transfer Impact Assessment (TIA) process must be carried out prior to such transfer. In relation to TIA processes, please contact Evac data protection organization. Also, a DPA must be in place.

  Example: *Evac sources services from third-party suppliers from China. Such service includes processing of Evac's personal data. Sourcing must have DPA in in place as well as carry out the TIA process.*

6. Individual rights

Individuals have many rights with regards their personal data, including:

Right of access – individual is entitled to have information concerning the personal data that is undergoing processing as well as a copy of such data.

Right to rectification – individual has the right to have any inaccuracies related to his/her personal data corrected.

Right to withdraw consent (when processing is based on consent) – for a consent to be valid, it needs to be withdrawable, and the individual has the right for such withdrawal at any time.

Right to data portability – under certain conditions, the individual may require his/her data to be ported to him-/herself or to another company in a commonly used machine-readable format.

Right to object – the individual has the right to object to certain processing, such as processing for electronic direct marketing, upon which the processing shall cease.

Evac shall ensure that individuals can effectively exercise their rights. Evac data protection organization shall be informed when an individual makes any of the abovementioned or any other requests relating to his/her personal data. Seek advice from Evac's data protection organization if you are uncertain about the individual's request and the necessary actions.

7. Further information

For further information and instructions, you may contact Group CFO, Group ISO or Group General Counsel.