EG-POL-010-ICT
Effective date 1 Nov 2026

Evac Group Oy

Evac Group Data Protection Policy

Table of Contents

Table of Contents 2

1. Introduction 4

2. Relevant data protection concepts 4

3. Purpose 5

4. Organisation and governance of data protection 5

5. Data protection principles 6

5.1 General 6

5.2 Lawful, fair and transparent processing 6

5.3 Accountability 8

5.4 Data security 8

5.4.1 Confidentiality 8

5.4.2 Appropriate security measures 8

5.4.3 Data breaches 9

6. Data disclosures and transfers 9

6.1 Disclosure to authorities 9

6.2 Transfer to external parties 10

7. Individual rights 10

8. Data protection impact assessment 11

9. Personal data on social media platforms 11

10. Use of cookies on websites and apps 12

11. Reporting concerns and consequences of violation 12

12. Further information 12

13. Review and follow-up 12

Revision history 13

1. Introduction

Evac Group Oy and its group companies ("Evac" or "Company") collect, store, transfer, erase and otherwise process various types of information concerning its employees, business contacts, customers and other individuals (data subjects) 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's personal data processing activities.

Each employee, director and member of the Board of Directors must understand and comply with this Policy. Persons 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.

We also expect our partners to comply with data protection laws and similar principles as set out in this Policy.

2. Relevant data protection concepts

Controller	When Evac 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 natural person whose personal data is being processed.
Joint controllers	Sometimes two or more organisations 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	Any information relating to a data subject, *e.g.*, a name, an identification number, location data, an online identifier or identifiers related to the data subject's physical, physiological, genetic, mental, economic, cultural or social identity.
Processing	Any operation performed on personal data, for instance collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise

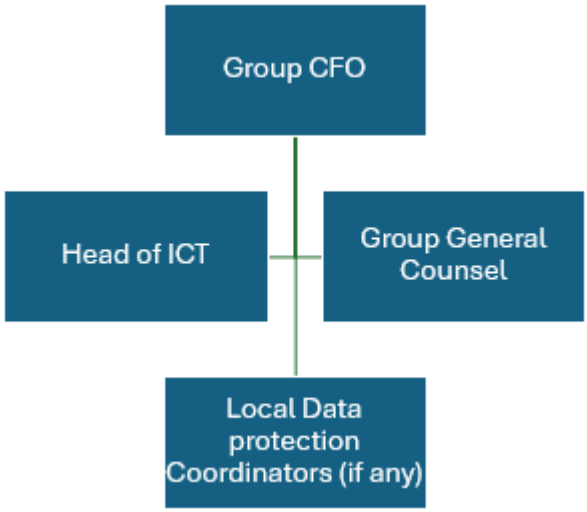
	making available, alignment or combination, restriction, erasure or destruction.
Processor	A company processing personal data purely on behalf of, and under the instructions, of another company. When Evac engages third parties to provide it with services *e.g.*, IT suppliers or payroll services, these service providers usually act as processors (and Evac acts as the controller). Controller-processor relationships must be governed by a data processing agreement.
Special categories of personal data	Sensitive data that merits higher protection and is generally prohibited from processing, unless specific derogations apply. Such data 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. Purpose

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

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

4. Organisation and governance of data protection



Group CFO has the overall coordinating role for all data protection matters within the Company. For cyber and information security matters, the ownership lies with the Group ICT team. Company 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 EU General Data Protection Regulation (GDPR).

Data protection matters are regularly discussed among Group CFO, Head of ICT and Group General Counsel. Group CFO reports material data protection matters to the Group Leadership Team ("GLT"). GLT escalates matters to the Board of Directors of the top holding company 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 authorised processors of Evac's personal data shall have appropriate expertise and awareness of requirements relating to the 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.

5. Data protection principles

5.1 General

General data protection principles form the foundation of personal data processing within Evac. Whenever the business functions within Evac's organisation are processing personal data, it is their responsibility to ensure that these principles are fulfilled, with the support from the data protection organisation described in Section 4.

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.

5.2 Lawful, fair and transparent processing

When processing personal data, the controller must:

(i) **Transparency**: ensure that individuals are aware of how their personal data will be processed.

- *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.

(ii) **Appropriate legal grounds:** ensure the existence of appropriate legal grounds for the processing of personal data, such as Evac's legal obligation, the data subject's valid consent, contractual necessity or Evac's legitimate interest.
Further, ensure the existence of legal grounds for processing any special categories of personal data that necessitate higher protection and are generally prohibited from processing.

- *Example*: Personal data cannot be collected "just in case" or for purposes to be defined in the future. Appropriate legal grounds must exist for the data to be processed. For 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 fulfilment of that contract.

(iii) **Necessity:** ensure that, once a legal ground for processing exists, only adequate and relevant personal data necessary for the specific purpose is processed. Consider why the data is collected – if there is no clear and justified business reason for processing the personal data, it shall not be processed.

- *Example*: Collection of employee data may be necessary for, *e.g.*, the management of Evac's (employer) and employees' rights and responsibilities in relation to the employment relationship.

- *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 do not always require data on the level of specific individuals.

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

(iv) **Accuracy:** ensure that the personal data being processed is accurate and kept up to date (inaccurate personal data to be erased in a secure manner or rectified without delay).

(v) **Storage limitation:** ensure that personal data is not being retained for longer than is necessary for the purposes for which the data are being processed, being mindful that law may impose an obligation to retain data in certain circumstances (*e.g.,* financial data and job certificates).

(vi) **Consent when using tracking technologies:** when profiling customers or using targeted advertising using tracking technologies such as cookies or tracking pixels, ensure that the customers have consented to the profiling and/or targeted advertising.

(vii) **Ask for help:** seek advice from data protection organisation, if you are uncertain of the legitimacy of personal data processing.

(viii) **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 entering into a 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 supplier. 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. As 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.

5.3 Accountability

When personal data processing activities are planned or personal data is already processed, the controller needs to document everything that might be relevant for Evac to demonstrate accountability with regards to its data processing activities.

5.4 Data security

5.4.1 Confidentiality

Evac shall ensure that appropriate processes, procedures, and non-disclosure agreements are in place so that persons authorised to process personal data are subject to a duty of confidentiality and process such data only as necessary for the performance of their duties. See also the Company's Confidentiality Policy.

- *Example*: All employment and supplier agreements need to have appropriate confidentiality clauses.

5.4.2 Appropriate security measures

Appropriate technical and organisational measures shall be implemented to protect confidentiality, integrity and availability of personal data in accordance with Evac's 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 considering 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, the controller 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.

5.4.3 Data breaches

A personal data breach entails a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Employees and other authorised persons shall immediately report any personal data breach or comparable incident to the Group CFO, Head of ICT or Group General Counsel.

Where a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, Evac shall notify the relevant data protection authority in accordance with applicable legislation and no later than 72 hours after becoming aware of the breach. Where the personal data breach is likely to result in a high risk to individuals, Evac shall also communicate the breach to the affected individuals without undue delay.

Evac may also be required to notify other third parties of a data breach, such as insurance companies or other relevant parties, in accordance with contractual obligations.

- *Example*: Accidental disclosure of personal data to an unauthorised party constitutes a personal data breach and shall immediately be notified to Group CFO, Head of ICT or Group General Counsel.

- *Example*: If there is a suspicion that personal credentials (such as passwords) have been misused to gain unauthorised access to Evac's applications or data sources, the incident shall be immediately reported to the Group CFO, Head of ICT or Group General Counsel.

6. Data disclosures and transfers

6.1 Disclosure to authorities

To ensure safety and confidentiality of personal data controlled by Evac 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.

6.2 Transfer to external parties

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

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

Prior to transferring any personal data to a processor, necessary contractual measures need to be in place. Data processing agreement templates provided by the Group Legal team 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 to guarantee that data is managed and processed appropriately by the outsourcing (external) partner.

- *Example*: When personal data processing is centralized to Evac headquarters (*e.g.*, CRM application), it is seen as an outsourcing relationship between Evac and the country organisation if the ownership of the data remains local. In such a scenario, an intra-group DPA 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, you should contact Evac's data protection organisation. Also, a DPA must be in place.

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

7. Individual rights

Data subjects have many rights with regard to their personal data, including:

(i) **Right to access** – the data subject is entitled to have information concerning their personal data that is being processed as well as a copy of such data.
(ii) **Right to rectification** – the data subject has the right to have any inaccurate personal data concerning them corrected.
(iii) **Right to withdraw consent** (when processing is based on consent) – for a consent to be valid, it needs to be withdrawable, and the data subject has the right for such withdrawal at any time.
(iv) **Right to data portability** – under certain conditions, the data subject has the right to receive personal data concerning them in a structured, commonly used, and machine-readable format and to transmit that data to another controller.

(v) **Right to object/opt-out** – the data subject has the right to object to and opt-out of certain processing, such as processing for electronic direct marketing, upon which the processing shall cease.

(vi) **Right to erasure** – under certain conditions, the data subject has the right to request the erasure of personal data concerning them (*e.g.*, where the processing is no longer necessary, withdrawal of consent and where there are no legal grounds for the processing).

(vii) **Right to restriction** – for instance in situations where the accuracy of personal data is contested by the data subject.

Evac shall ensure that the data subject can effectively exercise their rights. Evac must inform on any action taken on a request to the data subject without undue delay and in any event within one month of receipt of the request. The time limit may, if necessary, be extended by two months if Evac informs the data subject of the extension and the reason for the delay at the latest one month after the request was received. Evac is under a duty to take all reasonable actions to check the identity of the data subject.

Evac data protection organisation shall be informed when the data subject makes any of the abovementioned or any other requests relating to their personal data.

Employees and other authorised persons shall seek advice from Evac's data protection organisation if there is uncertainty regarding a data subject's request or the appropriate actions to be taken.

8. Data protection impact assessment

Even if there is a valid legal ground to process personal data, Evac must first conduct a data protection impact assessment if it wishes to engage in data processing activities that are likely to result in high risks to the rights and freedoms of natural persons (*e.g.*, installing camera surveillance in office areas).

A data protection impact assessment is a process to help identify and minimise the data protection risks of a processing activity.

The Group General Counsel shall be consulted for further guidance and instructions regarding data protection impact assessments.

9. Personal data on social media platforms

Whenever Evac has accounts on social media platforms (*e.g.*, LinkedIn, 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 Evac is in control of such publications and has the possibility of making adjustments/delete such information.

Whenever Evac uses tools provided by a social media platform, *e.g.*, marketing or analytics tools, there is often a joint controllership between Evac and the social media platform.

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

10. Use of cookies on websites and apps

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

Whenever Evac uses cookies or similar tracking technologies 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, statistics 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 Evac'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.

11. Reporting concerns and consequences of violation

Employees and other authorised persons who become aware of, or suspect, a possible violation of law, regulation, or this Policy shall promptly report the matter to the Group CFO, Head of ICT or Group General Counsel.

Concerns may also be raised anonymously through Evac's whistleblowing system available at Whistleblowing - Evac. Evac 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 will be considered a violation of Evac's Code of Conduct and will not be tolerated.

Evac does not tolerate any illegal or unethical behaviour. Violations of this Policy are likely to damage Evac's brand and reputation. Failure to comply with this Policy may result in disciplinary action proportionate to the violation, including, but not limited to, termination of the employment.

12. Further information

Further information and instructions may be obtained from the Group CFO, Head of ICT or Group General Counsel.

13. Review and follow-up

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

Revision history

REV. NO.	DESCRIPTION	AUTHOR	APPROVER	APPROVAL DATE	EFFECTIVE DATE
1	First release	Sampo Kättö	Board	22 Nov 2022	22 Nov 2022
2	Amendments	Sampo Kättö	CEO	10 Feb 2025	10 Feb 2025
3	Amendments	Sampo Kättö	The Board of Directors of CAVE BidCo Oy	23 Sep 2026	1 Nov 2026



Evac is the world's leading provider of integrated water and waste management systems, as well as corrosion-protection systems for the marine, offshore, and building industries. With offices across four continents and representatives in more than 70 countries, we are close to our customers wherever they are. We contribute to a better environment and cleaner seas by helping our customers eliminate waste, conserve water, and mitigate emissions. Our ambitious target is to enable a future with no waste.

Read more about our solutions
evac.com

evac
nothing to waste

Innovative water and waste technologies on land and sea driving a future with no waste.