Information Security and Personal Data Policy

CASTELLUM

This policy was adopted by the Board of Directors of Castellum AB (publ) on 29 April 2026

Contents

1. Background

This Information Security and Personal Data Policy states the general principles for the procedures of Castellum AB (publ) ("**Castellum**") routines for work related to information security and processing of personal data. This policy aims to protect Castellum's information, systems and infrastructure, against threats and risks that may affect our operations and the trust of our stakeholders. The policy serves to support the organisation and every employee must be informed of how we work with information security and how personal data are to be processed at Castellum. Further information on procedures can be found in our internal governing documents.

Situations covered by this policy could, for example, be the processing of employees' personal data in the employment context or processing a tenant's personal data to fulfil our obligations in accordance with the landlord-tenant relationship. All personal data processing at Castellum or when performed by a third party on behalf of Castellum is to follow applicable regulations and any personal data breaches are to be dealt with promptly. A high level of information security is an important component in this context, and an incident in our network and information systems may result in damage to both personal data and other information assets.

The purpose of this policy is to ensure a high level of information security, i.e., the confidentiality, integrity, and availability of information, and thereby also the proper processing of personal data. Any violation of this policy may prejudice the individual's security and risks damaging Castellum's brand. Furthermore, it may result in major economic consequences with risk of sanctions, which would harm Castellum's financial position and earnings.

2. Document owner

Castellum's Information Security and Personal Data Policy is to be revised on a regular basis and adopted by the Board at least once each year. The Chief Legal Officer (Erika Taube) of Castellum is the document owner and responsible for the policy.

3. Scope

Castellum protects each individual's personal privacy and safeguards that all personal data are processed in accordance with applicable regulations, which is essential in order to maintain Castellum's trust as employer and in relation to tenants. A high level of information security is essential in this work and, more generally, for protecting information assets in our systems and networks.

The Information Security and Personal Data Policy encompasses and is applicable to all companies in the Castellum Group and to all individuals who are employed or otherwise work in the Castellum Group or perform duties for companies in the Castellum Group.

4. Applicable legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council (the "**General Data Protection Regulation**") is directly applicable in Sweden. Castellum's data protection activities are to be consistent with the General Data Protection Regulation and fulfil the requirements laid down for personal data processing and the principles for such processing.

In addition, Castellum must comply with the applicable legislation in the area of information security and data protection prevailing at any given time.

5. Information security

5.1 Overall Purpose

Castellum's operations shall be structured in a way that ensures a high level of information security, with implemented routines to protect network and information systems from incidents, as well as to ensure correct authorization and classification of information assets. The key principles are:

- **Confidentiality:** Ensuring that sensitive information, such as customer data and financial reports, is protected from unauthorized access.
- **Integrity:** Preventing unauthorized alterations of information and ensuring that data is accurate and reliable.
- **Availability:** Ensuring that information and systems are accessible to authorized users when needed to support operations.

5.2 Risk Management

Castellum shall work with information security from an all-hazards perspective, meaning that the work shall be structured around identifying, analyzing, and minimizing risks in our systems. Regular risk analyses shall be conducted to identify unauthorized access and minimize the risk of ransomware attacks, operational disruptions, and data leaks.

5.3 Business Continuity and Crisis Management

Castellum shall have routines in place to maintain operations during crises. This includes backup, restoration, and recovery of information assets. Regular restoration tests shall be performed, and an action plan shall be in place for managing interruptions and operational disturbances.

5.4 Network Security

Castellum's networks shall be equipped with protective security functions to prevent unauthorized access. Continuous efforts shall also be made to protect the organization against malicious code and unauthorized software.

5.5 Security Testing

Castellum shall continuously conduct security tests to identify weaknesses in information security. The tests shall ensure, among other things, that systems are updated, that configurations address published vulnerabilities, and that selected technical security measures for systems and the digital environment are implemented. Deviations shall be documented and addressed with concrete improvement actions.

5.6 Training

All employees shall receive annual training in information security to increase awareness and reduce the risk of incidents. Group management, together with the IT function, shall regularly evaluate whether additional measures are needed based on completed risk analyses.

5.7 Handling of Information Security Incidents

Castellum shall have clear routines in place to detect and manage incidents. If employees or others performing assignments for Castellum suspect that an incident has occurred, it must be reported immediately to Castellum's IT function. Incidents shall be documented to ensure traceability and follow-up. The IT function shall report serious incidents to Castellum's compliance function, which is also the Chief Legal Officer of Castellum. If the incident involves personal data, the reporting obligations in section 6.10 also apply.

5.8 System Management Organization and Security Classification

Castellum has implemented routines for managing data protection and information security within system management to ensure that our information assets are protected. System management is structured so that each function has an object owner (the function's manager) with overall responsibility for the function's systems. Before entering into an agreement to implement a new system, an analysis of the system's functionality, technology, and security shall be conducted to ensure that it meets Castellum's information security requirements. If personal data will be stored in the system, a data processing agreement must also be entered into in accordance with section 6.4.

The object owner shall also be the information owner and ensure that all information assets within the function are correctly classified according to the *IT Security Guidelines*. This means that the information owner has overall responsibility for deciding on classification and appropriate protection levels. Within property management, the respective regional CEO is the information owner. Castellum's employees shall continuously classify information assets according to the decisions of the respective information owner.

6. Processing of personal data

6.1 Legal principles

Before commencing each personal data processing operation, Castellum must verify compliance with the following principles:

a) **Lawfulness, fairness and transparency –** There shall always be a legal basis (refer to Point 6.2 below) for personal data processing and it shall be accurate and marked by transparency.

b) **Purpose limitation** – It shall be ensured that the purposes of the personal data processing are expressly stated and that these are legal and that the data are not further processed in a manner that is incompatible with those purposes.

c) **Data minimisation** – The personal data processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) **Accuracy** – The personal data must be accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that personal data which are inaccurate are rectified or erased.

e) **Storage limitation** – Personal data must be stored for no longer than is necessary for the purposes for which the personal data are processed.

f) **Accountability** – The personal data shall be protected by appropriate technical and organisational measures to ensure they are not accessible to unauthorised parties, destroyed or damaged.

6.2 Legal basis

A legal basis is required in order to process personal data, as specified in the General Data Protection Regulation. In practice, four legal bases are relevant to Castellum, of which Castellum bases its personal data processing on the following points:

(i) **Consent** – The consent by a data subject to processing of their personal data constitutes a legal basis. Consent must always be freely given and shall be revocable. Consent must not be used in situations when there is an imbalance between the parties, such as relations between an employee and employer.

(ii) **Performance of contract** – When it is necessary to process personal data for the performance of a contract to which the data subject is party, for example to allow Castellum to fulfil its commitments in accordance with an employment contract and to a pay salary.

(iii) **Compliance with legal obligations** – When it is necessary for compliance with a legal obligation, for example when Castellum in its capacity as employer has a legal obligation to provide information on taxation to the tax authority.

(iv) **Balancing of interests** – When balancing interests it is decided that the processing is necessary for the purposes of Castellum's legitimate interests and that such interests override the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

6.3 Transparency and information disclosure

The data subject is to be informed if their personal data will be processed, which company or companies that will process the data and for which purpose. Such information must also be provided as regards the use of cookies.

6.4 Processor agreement

Where an external party processes personal data on behalf of Castellum or where Castellum processes personal data on behalf of an external party, Castellum must enter into a processor agreement with the relevant party. The processor agreement is to be consistent with this policy.

6.5 Processing of special categories of personal data

As a general rule, processing of personal data revealing, for example, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sexual orientation is prohibited. Castellum only processes special categories of personal data when there is explicit support in the General Data Protection Regulation.

6.6 Data protection impact assessment

Where a type of processing is likely to result in a high risk to the integrity of natural persons, Castellum must perform an impact assessment prior to the start of processing activities. Castellum's data protection officer must be involved in the impact assessment (see point 6.9 below).

6.7 Internal records of personal data processing

Each Castellum company that acts in the capacity of controller is responsible for complying with the General Data Protection Regulation and other applicable data protection laws and shall also be able to demonstrate compliance with the General Data Protection Regulation. Each controller achieves this by maintaining a record of all processing performed by Castellum within the framework of its operations.

6.8 Rights of the data subject

The General Data Protection Regulation sets out a number of fundamental rights that the data subject is entitled to exercise in relation to Castellum's personal data processing. Castellum shall have procedures in place to ensure that the data subject's rights are safeguarded.

a) **Right to rectification, erasure and restriction** – Reasonable measures should be used to ensure that inaccurate personal data are rectified, made complete or erased without undue delay.

b) **Right to object** – The data subject has the right to object to Castellum's personal data processing where it is based on a balancing of interests, see point 6.2 (iv) above.

c) **Right of access** – The data subject has the right to obtain from Castellum confirmation as to whether or not personal data are being processed and, where that is the case, access to the personal data by receiving a copy of the personal data processed.

d) **Right to data portability** – Castellum shall, at the request of the data subject, provide the personal data processed that concern the data subject.

e) **Right to withdraw consent** – The data subject has the right to withdraw their consent at any time, see point 6.2 (i) above.

6.9 Data protection officer

Castellum has appointed a data protection officer to perform the tasks set out in the General Data Protection Regulation. This includes carrying out an annual review of Castellum's compliance with the General Data Protection Regulation, taking part in impact assessments, contacting and cooperating with the supervisory authority and answering questions or requests from data subjects (see point 6.8 above).

6.10 Management of personal data breaches

Where an employee or other party performing duties for Castellum suspects that a personal data breach has occurred this must be immediately reported to Castellum's data protection team. The data protection team will process a report urgently and involve the functions at Castellum required to assess the scope of the breach. The data protection team will also contact Castellum's data protection officer who is responsible for submitting any report to the supervisory authority. If deemed necessary, the supervisory authority must be notified without undue delay and within 72 hours after Castellum was made aware of the breach.

Castellum shall document all personal data breaches, even those where notification to the supervisory authority is not required.

Information about the breach shall in some cases be given to the individual to whom the personal data relates. This assessment is made by Castellum's data protection team together with Castellum's data protection officer.

Castellum is to provide annual training to ensure that all employees are informed about applicable legislation and Castellum's procedures for managing personal data breaches.

7. Breaches of the policy

Any breach of this policy is to be reported to Castellum's Chief Legal Officer, who will in turn inform the Board of Directors of Castellum.

Persons who are uncertain as to how Castellum's Information Security and Personal Data Policy is to be interpreted or how the regulations are applicable, can contact Castellum's IT-function or data protection team for guidance.

Appendix 1 – Definitions under the General Data Protection Regulation

Definitions used in this policy are intended to have the meanings specified in the General Data Protection Regulation:

A. "*Processing*" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as 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.
B. "*Personal data*" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
C. "*Controller*" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
D. "*Personal data 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.