



Data Privacy Policy

Classification: PUBLIC
Version: 1.0

2023-04-18

Table of Contents

1 PURPOSE AND SCOPE 3

1.1 PURPOSE 3

1.2 SCOPE..... 3

2 DATA PRIVACY STANDARDS 6

2.1 PRINCIPLES OF DATA PROCESSING 6

2.2 LEGAL BASIS FOR DATA PROCESSING..... 6

2.3 RIGHT OF INFORMATION AND OBJECTION..... 7

2.4 ACCESS RESTRICTIONS AND CONTROLS 9

2.5 SECURITY 9

2.6 DATA TRANSFERS..... 9

3 GOVERNANCE..... 11

4 REPORTING OF VIOLATIONS..... 12

4.1 REPORTING OF VIOLATIONS..... 12

4.2 BREACH NOTIFICATION..... 12

5 OVERSIGHT 13

5.1 SELF-ASSESSMENT..... 13

5.2 RISK IDENTIFICATION 13

5.3 AUDIT 14

6 COMPLAINTS..... 15

7 CHANGE LOG 16

7.1 CHANGE LOG..... 16

7.2 DOCUMENT INFORMATION..... 16

1 Purpose and Scope

1.1 Purpose

As an IT Service provider, it is essential for Aeven to respect and protect data privacy. On behalf of our customers and within the Aeven we process data on a regular basis - a substantial portion of which is Personal Data.

This Data Privacy Policy sets out the standards and the principles, which Aeven collects, uses, stores and processes Personal Data. This Data Privacy Policy is based on the European Union General Data Protection Regulation 5419/16 (GDPR).

Personal Data must be processed in accordance with these standards and principles as well as in accordance with the instructions and requirements set out by Aeven's customers, in order to ensure the safety of the data and the integrity of the individual data subjects concerned by any processing carried out by Aeven or on behalf of others.

Aeven's processing of Personal Data must always adhere to applicable data privacy legislation; primarily the GDPR.

1.2 Scope

This Data Privacy Policy is a minimum standard applicable to all entities and employees of Aeven. Local management in the Aeven entities is responsible for the implementation of any local regulatory requirements.

Aeven will safeguard its customers' data, including Personal Data, with the same diligence and care as its own data.

The following definitions used in this Privacy Policy are:

Term	Definition
Data Controller	A natural or legal person (entity), public authority or any other body which alone or jointly determines the purposes and the means of the processing of Personal Data. The Data Controller is the main responsible entity for data privacy compliance, including inter alia compliance with applicable national and EU law.
DPO	Data Protection Officer. See Section 3 and 6.

Term	Definition
Data Processing	<p>Data processing is a central term in data privacy. It is very broadly understood and will apply in most instances where personal data is used in any way or form.</p> <p>Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, is considered data processing.</p>
Data Processor	A Data Processor is a natural or legal person, public authority, agency or any other body which processes Personal data on behalf of a Data controller.
Data Subject	<p>An identified or identifiable natural person (as opposed to a legal person) to whom Personal Data can be linked. In the context of this Data Privacy Policy the Data Subjects will typically fall into these categories:</p> <ul style="list-style-type: none"> • Persons whose data are processed by Aeven's customers in the course of their business (e.g., their customer data). • Aeven's customers' employees (e.g., employees in the customers' IT departments interacting with Aeven employees or systems). • Aeven employees. • Representatives of suppliers or partners.
Data Transfer	Disclosure, transmission of or making Personal Data available in any way or any form, including the mere access, to third parties.
EU Model Clauses	The EU model clauses are a set of standard contractual terms adopted by the European Commission. The EU Model Clauses constitute a standard data transfer agreement which allows Data Transfer to entities located outside the EU/EEA.
GDPR	EU Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Aeven	Aeven as a whole or an individual entity in the Aeven companies as the case may be. Aeven entities are all wholly owned and controlled subsidiaries of the parent company in the Aeven company, Aeven incorporated in Denmark.

Term	Definition
Personal Data	Any information, which can be linked to an identified or identifiable natural person. Such an identification link can be either direct or indirect. This makes it a very broad category of data, which is applicable in almost all instances where data is included as element of IT deliverables.
QPoint	Quality Management in IT: Aeven quality management system.
Sensitive Personal Data	<p>A subset of Personal Data that encompasses the following data:</p> <ul style="list-style-type: none"> • Racial and ethnical background • Political, religious or philosophic persuasion • Union affiliation • Medical records • Data concerning health • Data concerning sex life • Genetic and biometric data

2 Data Privacy Standards

2.1 Principles of Data Processing

Aeven has adopted the following principles of Data Processing, which shall always apply when Aeven is the Data Controller:

- Data Processing must have a legal basis.
- Data Processing must adhere to good privacy and industry practices.
- The Data Processing must be done with a clear purpose.
- The Data Processing must not extend beyond the purpose.
- Appropriate organizational and technical security measures must be applied in the Data Processing in order to prevent unlawful or unauthorized access, disclosure or destruction.
- The accuracy and authenticity of Personal Data must be ensured.
- Access must be restricted to ensure compliance with the principles set out above.
- Data Processing must be based on documented agreements between the Data Controllers and the Data Processors.
- International Data Transfers must be carried out in accordance with the EU Model Clauses or similar arrangements giving the Data Subjects the same degree of protection as if the Data Processing were carried out within the EU/EAA.

When Aeven acts as a Data Processor on behalf of its customers, Aeven will endeavor to ensure the above principles to the extent this is comprised by the instructions provided to Aeven and concluded between Aeven and its customers.

2.2 Legal basis for Data Processing

When acting as a Data Controller Aeven must ensure that its Data Processing is based on one of the following legal grounds:

- The Data Subject's consent, which must be freely given, explicit and informed.
- The Data Processing is necessary for the performance of contractual obligations between Aeven and the Data Subject.
- The Data Processing is necessary to ensure compliance with Aeven's legal obligations.

- The Data Processing is in the vital interest of the Data Subject.
- The Data Processing is necessary due to a public interest.
- The Data Processing is necessary to pursue legitimate interests of Aeven or a third party and when this interest is not contravened by the rights and freedoms of the Data Subject.

Further, when acting as a Data Controller with respect to Sensitive Data, Aeven must ensure that the Data Processing is based on one of the following legal grounds:

- The Data Subject's consent, which must be freely given, explicit and informed; or when the Data Subject is not able to consent, in order to safeguard the Data Subject's vital interests.
- The Data Processing is necessary for complying with or exercising rights on the applicable employment, social security and social protection law.
- The Data Processing is necessary for medicinal or diagnostic purposes.
- The Data Subject has publicized the information (however, Aeven must in this regard still adhere to the other applicable data privacy standards including this Data Privacy Policy, and in particular ensure that there is a legal basis).
- The Data Processing is necessary in order to exercise legal rights or claims of Aeven.
- The Data Processing is specifically permissible or otherwise required under local law.

2.3 Right of Information and Objection

Data Subjects shall have the following rights set out in this Section 2.3, which must be exercised in accordance with the procedure in Section 6 below. The obligations of Aeven differ depending on Aeven's role as either Data Controller or Data Processor acting on behalf of a third party Data Controller.

Aeven as Data Controller:

When Aeven is the Data Controller, Aeven will (to the extent reasonably possible) provide the Data Subjects with the following information insofar it is necessary for the Data Subject to exercise its rights under the GDPR, local law and this Data Privacy Policy:

- The identity of the Data Controller (that is, the relevant Aeven entity).
- The purpose and the legal basis of the Data Processing, including the legitimate interests pursued by Aeven when the legal basis is a legitimate interest.

- The recipients of the data.
- Data Transfers to entities outside the EU/EEA and the legal basis for such transfers.
- The Data Subject's right to complain as set out in Section 6 below.

The specific Data Processing activities carried out by Aeven are described in further detail in the privacy notices issued by Aeven either on the Aeven website or communicated to the Data Subjects in relation to specific Data Processing activities.

Data Subjects shall have, upon request, the following rights with respect to the Data Processing:

- Right of Access (confirmation to the data subject that Personal Data is processed, access in form of a copy of the data relating to the Data Subject).
- Right of Rectification (the right to change data)
- Right to be Forgotten (the right to have data deleted)
- Right to Restriction of Processing (right to have certain processing activities suspended)
- Right to Data Portability (right to have data delivered in a machine-readable format)
- Right to Objection (right to have certain processing activities limited).
- Right to Limit Automated Decision-making.
- Right to withdraw consent (if the processing is based on consent as the legal basis)

All such requests shall be made according to the procedure in Section 6 below. The rights may be subject to conditions or restrictions in certain instances, depending on such circumstances as the Data Processing, the purpose, the legal basis and the retention requirements.

Aeven as Data Processor:

When Aeven acts as Data Processor on behalf of a third party Data Controller, the obligation to inform the Data Subject rests with the said Data Controller. When a request from a Data Subject concerns a third party Data Controller, Aeven does not have any legal basis (inter alia due to obligations of confidentiality) to divulge information to the Data Subject. Aeven will therefore forward such requests without undue delay to the Data Controller and assist the Data Controller (to the extent reasonably possible) in complying its obligations with the Data Subject.

2.4 Access restrictions and Controls

Aeven has adopted the following definition of access and restrictions extending to all systems and types of data including Personal Data.

- Access to data must be limited to the personnel resources that need to have the access to perform their services.
- For specific types of data specific restrictions may apply which prevent or limit the access to locations outside the EU/EAA or even to specific countries in the EU/EAA and such access restrictions must be reflected in Aeven's service design.

2.5 Security

In order to safeguard Personal Data and to ensure and enforce the access restrictions set out in Section 2.4 above, appropriate technical and organizational security measures must always be taken to prevent the accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure of or access to data.

Compliance relies on a combination of technical and organizational security measures:

- Technical access management and technical security
- Procedures and rules
- Control and traceability ensuring enforceability, documentation and the possibility to investigate possible breaches.

2.6 Data Transfers

Aeven has a global presence, including major operations centers in Denmark, the Czech Republic, and the Philippines. Aeven therefore engages in Data Processing in the capacity as Data Controller and as Data Processor to third party Data Controllers (Aeven's customers) in different countries and with Personal Data from different countries of origin. Aeven is fully committed to ensuring that such Data Transfers have the requisite level of protection.

When engaging in Data Transfer whereby access to data is provided from one entity to another and where the receiving entity is located outside the EU/EEA, such Data Transfer requires a specific legal basis.

For Data Transfers involving Aeven data, i.e., data where one Aeven entity is Data Controller and another is the Data Processor, EU Model Clauses have been adopted between the Aeven entities.

For data transfers involving customer data, i.e., data where a customer is the Data Controller and an Aeven entity is the Data Processor or sub-processor, EU Model Clauses must be entered into between the customer entities acting in the capacity of Data Controllers and the relevant Aeven entities.

3 Governance

In order to ensure the effective implementation of and compliance with the Data Privacy Policy in the Aeven entities, Aeven has adopted the following governance:

The Aeven DPO is responsible for overseeing overall compliance with data privacy, including the Data Privacy Policy, as well as issuing guidance and counselling on matters of data privacy.

Aeven Legal provides legal business support, including in cooperation with the DPO, on matters concerning data privacy, in particular in relation to contractual matters.

Aeven Line of Business (LoB) — have the day-to-day operational responsibility for ensuring compliance with the Data Privacy Policy and Aeven's duties and obligations as a Data Processor.

Aeven HR is responsible for Aeven's compliance with the Data Privacy Policy when Aeven acts as a Data Controller, collecting and processing data about Aeven employees and applicants.

Other departments within Aeven are responsible for the compliance with the Data Privacy Policy and Aeven's responsibilities as Data Controller for the data collected, used, and processed by these departments.

As part of the overall commitment to quality within the Aeven organization, Aeven Quality & Security (Q&S) monitors and enforces compliance across Aeven.

Employees and external consultants with access to Aeven systems are required to be trained, stay updated, adhere to policies, processes, and procedures in QPoint when in contact with Personal Data.

4 Reporting of violations

4.1 Reporting of violations

Any breaches of the Data Privacy Policy are handled in accordance with Aeven's existing procedures for non-conformity in QPoint.

In addition to the ordinary internal lines of communication that can be used to report violations, Aeven has extended the scope of our whistleblower service to accommodate violations of this Data Privacy Policy and applicable data privacy law.

4.2 Breach notification

When a privacy data breach occurs where Aeven is Data Processor, Aeven will inform the Data Controller regarding the incident without undue delay.

When a privacy data breach occurs where Aeven is Data Controller, Aeven will inform the Supervisory Authorities and where applicable the Data Subjects in accordance with the requirements set out in the applicable data privacy law.

5 Oversight

5.1 Self-Assessment

Aeven conducts continuous self-assessment of the Data Privacy Policy.

Aeven conducts on at least a yearly basis a self-assessment based on data and information gathered specifically for the self-assessment (e.g., questionnaires or internal lessons learned) and the input derived from audits conducted as well as any registered complaints or non-conformities.

Furthermore, Aeven continues to monitor developments in legislation and regulatory practices, including in particular changes in data privacy practices adopted by the Supervisory Authorities and the relevant bodies in the EU.

The self-assessment process is anchored in the Governance set out in Section 3 above and is coordinated by the DPO.

5.2 Risk Identification

Risk identification is an integral part of the security measures set out in Section 2.5 above as well as the overall IT services management and quality management in Aeven, and is comprised of the following elements:

- Confidentiality (if information is revealed to unauthorized persons).
- Integrity (if data is changed by unauthorized persons).
- Availability (if system/data is not accessible during a given period).
- Information Classification.

Based on the above, appropriate measures and controls are established in order to reach an acceptable level of confidentiality, integrity and availability.

Aeven's procedures in Qpoint for security and incident reporting applies to all employees in Aeven working with supplying and maintaining compliance of IT services, systems, and data. Service specific risk identification can be provided as part of the services to customers.

5.3 Audit

Aeven audits the compliance with the Data Privacy Policy as part of the processes in QPoint for audits applicable to all aspects of Aeven's business and operation.

Internal Audit:

On a regular basis Aeven conducts internal audits of compliance with this Data Privacy Policy. The internal audits are conducted by Aeven Quality & Security department. The internal audit applies to Aeven's Data Processing in the capacity as Data Controller and Data Processor.

External Audit:

Aeven commits to external audits of its Data Processing, both in the capacity as Data Controller and Data Processor. The external audits may vary depending on the nature of the audit (i.e., does the audit concern Aeven as a Data Controller or Aeven as a Data Processor on behalf of third parties), as well as the contractual obligations between Aeven and its customers. Consequently, Aeven is subject to the following types of external audits:

- Customer audits, which are conducted by the customer on an ad hoc basis and pursuant to local legislation.
- Independent system audits: Audits performed on the basis of a customer requirement based on a specified scope (e.g., ISAE 3402).
- Agency audits: Audits or inspections conducted by Supervisory Authorities or other regulatory bodies.
- Standardization body audits: Audits pursuant to certifications by international standardization bodies (e.g., ISO).

6 Complaints

The following sets out Aeven's commitment to address complaints or requests for information from Data Subjects concerning Data Processing carried out by Aeven.

Complaints can be directed to Aeven DPO:

Aeven A/S
Att.: Aeven DPO
Østmarken 3A
DK-2860 Søborg
Denmark
Tel: TBA
Email: privacy@aevengroup.com

The Aeven DPO will initiate an investigation and ensure that any complaints from data subjects will be investigated thoroughly, and that the data subject will receive an appropriate and timely reply.

Direct complaints against Aeven — Aeven acting as Data Controller:

Direct complaints will be handled in accordance with the complaints procedure in Qpoint and if necessary raised as a non-conformity in accordance with the procedure for non-conformity.

Where necessary, Aeven will take corrective action to ensure that the principles in this Data Privacy are complied with.

Indirect Complaints — Aeven acting as Data Processor on behalf of a third party

Aeven will inform the relevant Data Controller and forward the complaint without undue delay and if the complaint concerns Aeven, assist the Data Controller (to the extent reasonably possible).

Direct complaints to the Supervisory Authority

Data subjects are entitled to complain to the Supervisory Authority.

7 Change log

7.1 Change log

Effective Date	Version	Change description	Author
2023-05-01	1.0	New document	NILI

7.2 Document information

Document version:	1.0
Criticality (N/A, base, critical, GxP):	Critical
Published date of this version:	2023-05-01
Effective date of this version:	2023-05-02
Author:	NILI
Owner:	NILI
Approved by:	MAJE, BPHE
QA Approval (only applicable on Critical and GxP Criticality):	