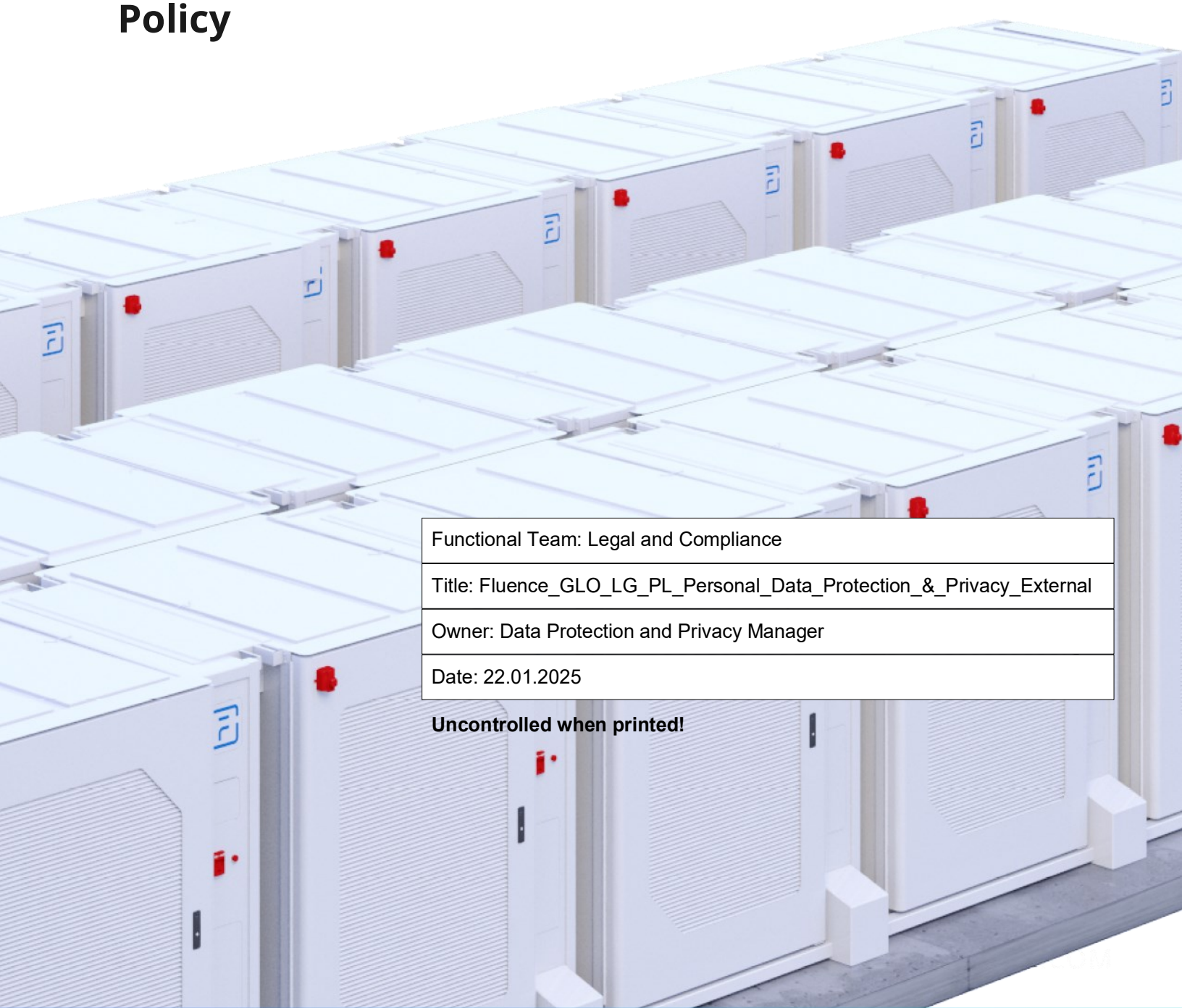
Personal Data Protection and Privacy (External)

Policy



Functional Team: Legal and Compliance
Title: Fluence_GLO_LG_PL_Personal_Data_Protection_&_Privacy_External
Owner: Data Protection and Privacy Manager
Date: 22.01.2025

Uncontrolled when printed!

Fluence Support Services can be contacted 24/7 at **+1 (703) 635-7631**.

Fluence Offices: Contact Us | Fluence - A Siemens and AES Company (fluenceenergy.com)

Revision History

Revision Number	Date	Authored By	Reviewed By	Approved By	Pages Affected
00	01/08/2024	Ercüment Ari	Markus Meyer	Markus Meyer	New

Table of Contents

1. Document Overview

Objective

Fluence is subject to applicable laws and regulations governing the handling and processing of Personal Identifiable Information (PII) in the jurisdictions in which it operates. Some of these regulations are territorial (e.g., GDPR) and others are local. While these laws and regulations vary across country jurisdictions, Fluence is required to observe and comply with both territorial and country specific regulations governing the protection of customer, prospective customer, and employee data shared with external entities, and to appropriately safeguard that data. Failure to comply with applicable laws and regulations may result in regulatory censure, loss of client confidence, damage to reputation, and financial liability.

This policy governs how Fluence handles and manages personal data in general.

Scope

This policy specifically addresses the management of Personal Data as distinct from other types of data. It is crucial to understand that references to "data" and its processing within this document pertain solely to Personal Data. This distinction is necessary because the lifecycle, management, and other requirements for Personal Data often differ from those applicable to other data types. Ensuring this differentiation is clearly understood and implemented is essential for compliance and effective data governance.

This policy applies to all Fluence employees and contractors who use, manage, design or implement Fluence's systems and data sources. The policy also applies to all hard copy and electronic information in the custody of Fluence related entities (which also applies under contractual obligations and the Supplier Code of Conduct), including but not limited to:

- Applicable Fluence entities and affiliates
- Partners
- Vendors / Suppliers

2. Terms and Definitions

Personal Data, Special Categorized Personal Data, Processing, Data Controller, Data Processor, Data Subject, Data Subject Access Request (DSAR), Consent, Data Breach mentioned in this document has the same definition as stated under **GDPR (General Data Protection Regulation).**

CPRA (California Privacy Rights Act): A law that enhances privacy rights and consumer protection for residents of the state of California, United States. It expands on the provisions of the California Consumer Privacy Act (CCPA).

Privacy Manager: Data Protection and Privacy Department's manager

Security Controls: Measures, both technical and administrative, employed by the company to protect and ensure the confidentiality, integrity, and availability of personal data. These controls encompass a range of practices including, but not limited to, encryption, access controls, physical security measures, and training. Their primary objective is to prevent unauthorized access, use, disclosure, alteration, and destruction of personal data, thus supporting the company's commitment to uphold GDPR and other related data protection regulations' requirements.

3. Roles and Responsibilities

Employees and Contractors, Data Protection and Privacy Manager, Business Privacy Leaders, Sales Teams, Marketing Team Responsibilities, Human Resources (HR) (HR Employees, HR Management), Compliance Management, Cybersecurity, Internal Audit, Legal, Work Counsel, Privacy Committee are responsible for data protection and privacy in company and their detailed roles are explained in intra company documents.

4. Data Privacy Principles

4.1 Lawfulness: Personal Information will be processed fairly and lawfully. Fluence will only collect and use personal information when it has lawful and serves a legitimate business purpose and Be transparent in its dealings with customers, prospects, employees, and applicants about what information it collects and processes about them.

4.2 Purpose Limitation: Personal Information will only be used by Fluence for the purposes for which it was originally collected and for which the individual was informed about.

4.3 Data Minimization: Personal Information that is only adequate, relevant, and not excessive will be processed, i.e.; Fluence will not ask for more information than it needs for the purpose for which it is collecting the information and will not record information that is not needed.

4.4 Accuracy: Fluence; will ensure Personal Information is kept accurate and up to date, update its records when an individual informs Fluence that his/her information has changed, periodically review and assess the quality.

4.5 Storage Limitation: Fluence will only keep Personal Information for as long as is necessary for the purpose(s) for which it was originally collected and personal data will be retained and securely disposed of in accordance with Fluence policies and standards.

4.6 Individual Rights: Fluence will observe the rights afforded to individuals under applicable privacy regulations governing the protection of personal data.

4.7 Integrity and Confidentiality (Security): Fluence, through its Data Privacy policies and procedures, shall ensure the implementation of appropriate technical and organizational measures to protect personal information from accidental or unauthorized disclosure, theft, damage, loss, alteration, or any other form of unlawful processing. Confidentiality and integrity controls shall be maintained to safeguard the protection of personal information (Refer to Annex 1 for specific details on Technical and Organizational Measures).

4.8 Data Transfer: Fluence will safeguard personal identifiers during the transfer to other countries/jurisdictions and third parties.

5. Data Collection Practices

5.1 Purpose of Collection

Fluence is committed to maintaining transparency regarding the purposes for which personal data is collected. Personal data shall be collected for the following reasons:

5.1.1 To refine and personalize user interactions on our digital platforms, ensuring a tailored and responsive experience.

5.1.2 To deliver and enhance products and services in alignment with the specific requests and expectations of our users and customers.

5.1.3 To facilitate clear and effective communication with users for the resolution of inquiries and to provide necessary support.

5.1.4 To perform essential business operations, including data analysis, audits, and optimizing internal processes for efficiency and innovation.

5.1.5 To conduct pre-employment assessments, ensuring candidates meet the necessary criteria and align with our organizational values and requirements.

5.1.6 To retain and utilize data in compliance with legal obligations post-employment termination, such as for tax purposes, reference checks, or to fulfill any ongoing contractual obligations.

5.1.7 To conduct surveys and gather feedback for the purpose of improving service offerings and addressing customer needs and preferences.

5.1.8 To strengthen corporate governance and risk management, ensuring responsible business practices and adherence to legal and regulatory standards.

5.1.9 To ensure compliance with legal and regulatory obligations, facilitate investigations, and address any potential legal issues or disputes.

5.1.10 To process employee data within the framework of legal statutes and requirements during the course of employment, the company adheres to the six lawful bases for data processing as stipulated by the General Data Protection Regulation (GDPR): consent, where employees have explicitly agreed to the processing of their personal data; contract, where processing is necessary for the performance of employment contracts; legal obligation, such as the necessity to process financial details to facilitate salary payments; vital interests, for instances where processing is required to protect an employee's life; public task, where processing is necessary for the company to carry out a task in the public interest or in the exercise of official authority; and legitimate interests, such as conducting performance evaluations, unless such interests are overridden by the rights and freedoms of the employees. Only collect and use personal information when it has lawful and serves a legitimate business purpose.

5.2 Types of Data Collected

Depending on interactions with the services, products, or platforms offered, the following types of data may be collected, including but not limited to:

5.2.1 Personal Identifiers: This encompasses full names, postal addresses, unique personal identifiers, phone numbers, email addresses, and other similar contact details.

5.2.2 Technical Data: Internet protocol (IP) addresses, login data credentials, browser type and versions, time zone settings, browser plug-in types and versions, operating system and platform, and other technologies on the devices used by the data subject to access the platforms are collected.

5.2.3 Employment and Background Data: For employment-related processes, this includes curriculum vitae, employment history, educational background, professional qualifications, and references.

5.2.4 Financial Data: Bank account details, payroll information, salary details, tax status, and other financial data relevant to employment and business dealings.

5.2.5 General Organizational Data: Comprehensive details about employees and contractors, which may include but are not limited to, performance data, disciplinary records, and workplace behavior data.

5.2.6 Profile and Usage Data: Preferences in receiving marketing communications, communication preferences, feedback, survey responses, as well as interactions with the website, products, and services, including the tracking of usage through cookies or similar technologies, are collected.

5.2.7 Sensitive Personal Data: Where necessary and with the data subject's consent, or as otherwise permitted by law, special categories of data, such as health data, may be processed.

5.2.8 Security and Compliance Data: Details that help us to ensure the security of our platforms, prevent fraud, and maintain compliance with legal obligations, including data for background checks and security clearances.

5.3 Special Categorized Personal Data (Sensitive Personal Data):

5.3.1 Principles for Processing:

Fluence shall only process sensitive personal data only in accordance with Article 9 of GDPR titled "Processing of special categories of personal data".

5.3.2 Safeguards for Processing Sensitive Personal Data: General data protection principles and safeguards are outlined in Annex-1 4. of this policy.

5.3.3 Individual Rights: Fluence will observe the rights afforded to individuals under applicable privacy regulations governing the protection of personal data. Responsibility and Compliance.

5.3.4 Fluence's Data Protection and Privacy Manager shall be responsible for overseeing and ensuring compliance with the processing of sensitive personal data within the organization. Any instances of non-compliance or potential breaches involving sensitive personal data shall be promptly reported to the Data Protection and Privacy Manager for investigation and appropriate action.

5.4 Methods of Collection

Fluence use a variety of methods to collect data, including:

5.4.1 Direct Interactions: Fluence obtain data such as identity, contact, and financial information directly from our users when they fill in forms on our website, sign up for services, or communicate with us through post, phone, email, or other direct interactions.

5.4.2 Automated Technologies: While users navigate our website, Fluence use cookies and other similar technologies to automatically collect technical data about their devices, as well as their browsing actions and patterns, ensuring users are informed and have control over their data.

5.4.3 Third Parties: Fluence may receive additional personal data about our users from third-party sources such as analytics providers, marketing partners, or credit reference agencies, as well as from publicly available databases, always ensuring that these sources are compliant with the GDPR.

5.4.4 Consent-Based Collection: Fluence collect data when users provide their consent for specific uses, such as subscribing to our newsletter or participating in marketing research.

5.4.5 Contractual Necessities: Some data is collected to fulfill our contractual obligations with our users, such as processing transactions or providing customer support.

5.4.6 Legal and Regulatory Requirements: Fluence collect data as required by law, such as for tax purposes, or to comply with regulatory inquiries and checks.

5.4.7 Legitimate Interests: Fluence collect data necessary for our legitimate interests, such as to improve our services, protect against fraud, or ensure network and information security, while carefully considering and respecting the rights and freedoms of our users.

5.5 Purpose and Legal Basis for Processing

5.5.1 Our legal basis for collecting and using the personal data described above will depend on the personal data concerned and the specific context in which Fluence collect it. Fluence will process personal data in accordance with Article 6 of GDPR titled “Lawfulness of processing”.

6. Data Sharing and Transfers

6.1 Purpose of Data Sharing and Transfers

Fluence recognizes the importance of personal data and values the trust of our stakeholders. Data sharing and transfers occur for specific operational requirements and always in accordance with applicable laws and regulations.

6.2 Internal Data Sharing

6.2.1 Departments: Data sharing within Fluence happens between various departments, ensuring smooth operations and effective service delivery. Such sharing strictly adheres to the principle of 'need to know', ensuring that only relevant data is accessible to specific teams or individuals.

6.2.2 Subsidiaries and Affiliates: For global operations, data might be shared with our subsidiaries and affiliates. This is done under inter-company agreements and standard contractual clauses ensuring the same level of protection as in the originating country.

6.3 Third-party Data Sharing

6.3.1 Service Providers: Fluence may share data with third-party vendors, consultants, and other service providers who perform services on our behalf. They are contractually bound to maintain the confidentiality of the information and use it only for the intended purposes.

6.3.2 Legal Requirements: Fluence might disclose personal data when it believes, in good faith, that such actions are necessary to comply with legal obligations, protect rights, or enforce our contractual agreements.

6.4 International Data Transfers

Given our global footprint, personal data may be transferred to and processed in countries other than the country of origin. Such transfers are undertaken with the following safeguards:

6.4.1 Adequacy Decisions: Transfers are made to countries that have been deemed by the European Commission to provide an adequate level of data protection. This ensures that the recipient country's data protection framework is equivalent to the standards set forth in the GDPR.

6.4.2 Standard Contractual Clauses: When transferring data outside the organization or to regions without an 'adequacy decision,' Fluence relies on standard contractual clauses approved by regulatory bodies.

6.4.3 Binding Corporate Rules (BCR): Fluence may in the future implement BCRs for intra-group transfers, which are a set of terms approved by European data protection authorities ensuring adequate protection.

6.4.4 Intercompany Agreement (ICA): For intra-group data transfers, Fluence employs an Intercompany Agreement (ICA), which ensures that all entities within the Fluence corporate structure adhere to consistent data protection standards. This agreement is designed to ensure compliance with GDPR requirements and to facilitate safe data transfers between Fluence entities, regardless of the country in which they operate.

6.4.5 Other Applicable Mechanisms: In the absence of the above, Fluence ensures other legally compliant mechanisms are in place before transferring personal data.

Risk and Mitigation Measures: Fluence recognizes the inherent risks associated with transferring personal data internationally. To mitigate these risks, we conduct thorough assessments and implement appropriate safeguards to ensure that data remains secure throughout the transfer process. Employees and stakeholders are encouraged to reach out to the Data Privacy Office for further information on the measures in place to protect their data

6.5 Consent, Control and DSARs

6.5.1 Before any unforeseen sharing or transfer that falls outside the scope of this policy, Fluence will obtain the explicit consent of the data subject.

6.5.2 Data subjects have the right to know and control where their data is transferred and can exercise this right as specified in the Data Subject

Requests Procedure. The request is a formal request by an individual to obtain confirmation as to whether their personal data is being processed and, if so, to gain access to that data and supplementary information. According to the GDPR, Fluence is required to respond to DSARs promptly and within one month of receipt.

7. Data Retention and Disposal

Fluence is committed to retaining personal data only for the duration necessary to fulfill the specific purposes for which it was collected, in alignment with legal, regulatory, and business requirements. After such time, the data will be securely and appropriately disposed of.

Fluence will abide by all applicable record keeping requirements. For further details including but not limited to Retention Periods, Review of Retained Data, Data Archiving, Secure Disposal Methods, Documented Procedures are included in the related retention procedure of Fluence.

8. Third-Party Processors and Suppliers

In the course of our business, Fluence may engage third-party processors, vendors, consultants and suppliers to provide various services. Fluence's measures for third party processors and suppliers are detailed in Annex-1.

9. International Considerations

9.1 Fluence operates in various jurisdictions worldwide. As a result, it is imperative for us to recognize and adhere to different international data protection regulations. This section highlights the key international considerations that inform our personal data protection and privacy practices.

9.2 Fluence operates in areas that falls under jurisdictions of EEA/EMEA especially Germany, United States of America, Australia, United Kingdom and acts in accordance with the related legislations.

9.3 In addition to the specific areas and respectable legislations mentioned, Fluence acknowledges the diversity of data protection laws across various global jurisdictions. Wherever operations occur, Fluence is dedicated to aligning our personal data protection and privacy practices with the respective local regulations. This includes, but is not limited to, respecting local data subject rights, ensuring lawful international data transfers

according to each jurisdiction's standards, and maintaining a high level of security for personal data. Fluence commits to ongoing monitoring and adjusting our compliance efforts in accordance with the evolving landscape of international data protection laws, ensuring that our practices remain at the forefront of data privacy excellence.

10. Data Protection and Information Security

In its strategic guideline Personal Data Protection and Privacy Policy, Fluence and affiliates have set itself the goal, among other things, of providing its employees and customers with the products and services to be delivered at the highest possible level of information security in compliance with the law. The technical and administrative measures are listed below:

10.1 Security Organization and Roles

Fluence has established a distinctive cross-sectional security organisation to ensure comprehensive protection of its own corporate information and data, as well as the data of its customers and clients.

10.2 Employee Training and Confidentiality Obligations

Employees are continuously informed and trained in the area of data protection and information security. In addition, all employees are contractually bound to data secrecy and confidentiality.

10.3 Confidentiality Agreements with External Parties

External parties who may come into contact with personal data in the course of their work for Fluence are obligated to maintain secrecy and confidentiality as well as to comply with data protection and data secrecy by means of a so-called NDA (Non-Disclosure Agreement) before they begin their work.

10.4 Group-Wide Data Protection

All affiliated companies of the Fluence group of companies within the EU or the EEA have concluded a joint framework agreement on data protection and commissioned data processing as a binding written legal instrument pursuant to Art 28 GDPR in order to ensure a uniformly high standard of data protection and data security across the entire group and to clearly regulate the rights and obligations for any commissioned data processing.

10.5 Technical and Organizational Measures, Security Standards and Certifications Listed under Annex-1.

11. Complaints and Redress Mechanisms

Fluence is committed to safeguarding personal data and upholding the highest standards of data privacy. If, however, a data subject believes that these standards have not been met, several mechanisms are provided to raise concerns and seek redress.

11.1 Internal Complaints Mechanism

11.1.1 Lodging a Complaint: If data subject have any concerns about how data subject's personal data is handled, data subject can lodge a complaint directly with our Privacy Manager using the contact details provided in the "Contact Information" section.

11.1.2 Resolution: Once a complaint is received, it will be reviewed within 30 days, and data subject will receive a formal response. If the investigation is complex, Fluence might require more time, but will keep data subject informed.

11.2 External Complaints Mechanism

11.3 Regulatory Authorities

In the event that a data subject is not satisfied with the resolution of their complaint or the manner in which Fluence has handled it after providing a formal response, the data subject shall have the right to lodge a complaint with the data protection regulatory authority in their jurisdiction..

11.3.1 International Redress: For cross-border data transfer issues or disputes, Fluence also adheres to international redress mechanisms as stipulated by regional regulations, ensuring that all data subjects, regardless of their location, have a path to redress.

11.4 Continuous Improvement

Fluence value feedback and treat all complaints as an opportunity to improve company policies and practices. All insights gathered from redress processes will be fed back into our ongoing policy reviews and updates.

12. Other

12.1 Enforcement

This policy represents the mandated rules, intentions and objectives endorsed by Executive Management with respect to the established controls and posture within Fluence.

13. Contact Information

13.1 For any questions, concerns, or clarifications regarding this Personal Data Protection and Privacy Policy, or to exercise data subjects's rights concerning personal data, please contact us through the following means:

Title:

Data Protection and Privacy Manager

Postal Address:

Fluence Energy GmbH, Schallershofer Str. 143, 91056, Erlangen, Germany

Adresse/Address:

Schallershofer Str. 143, 91056, Erlangen, Germany

Email Address:

For Germany: dpt_germany@fluenceenergy.com

For EMEA: dpt_eu@fluenceenergy.com

For Global: dpt_global@fluenceenergy.com

For Incidents (or potantials): dpt_ir@fluenceenergy.com

Telephone: +49 1733855973

In the event of any concerns regarding the data processing activities of the organization or the suspicion of a potential breach of data protection rights, it is recommended to first contact the Data Privacy Manager. Should the resolution be deemed unsatisfactory, the right to lodge a complaint with the relevant data protection supervisory authority in the respective jurisdiction may be exercised.

APPENDIX

TECHNICAL AND ORGANIZATIONAL MEASURES (TOMs)

The technical and organizational measures are implemented by Fluence in accordance with GDPR Article 32. They are continuously improved by Fluence according to feasibility and state of the art - not least also in terms of the active ISO 27001 certification - and brought to a higher level of security and protection.

1. Confidentiality

1.1 Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

Technical Measures	Organizational Measures
✓ Alarm system	✓ Key regulation / List
✓ Automatic access control system	✓ Reception / Receptionist / Gatekeeper
✓ Smart cards/transponder systems	✓ Visitors' book / Visitors' protocol
✓ Manual locking system	✓ Employee/visitor badges
✓ Doors with knob outside	✓ Visitors accompanied by employees
✓ Doorbell system with camera	✓ Information Security Policy
✓ Video surveillance of entrances	✓ Work instructions for operational safety
	✓ Work instruction access control

1.2 Logical Access Control

Measures suitable for preventing data processing systems from being used by unauthorized persons.

Technical Measures	Organizational Measures
✓ Login with username + strong password	✓ User permission management
✓ Anti-Virus Software Servers	✓ Creating user profiles
✓ Anti-Virus Software Clients	✓ Central password assignment
✓ Firewall	✓ Information Security Policy
✓ Intrusion Detection Systems	✓ Work instruction IT user regulations
✓ Use of VPN for remote access	✓ Work instruction operational security
✓ Encryption of data carriers	✓ Work instruction access control
✓ Encryption of smartphones	✓ Mobile Device Policy
✓ Automatic desktop lock	
✓ Encryption of notebooks / tablet	
✓ Two-factor authentication in data center operation and for critical systems	

1.3 Authorization Control

Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use and after storage.

Technical Measures	Organizational Measures
✓ Logging of accesses to applications, specifically when entering, changing, and deleting data	✓ Key regulation / List
✓ Automatic access control system	✓ Reception / Receptionist / Gatekeeper
✓ Smart cards/transponder systems	✓ Visitors' book / Visitors' protocol
✓ Manual locking system	✓ Employee/visitor badges
✓ Doors with knob outside	✓ Visitors accompanied by employees
✓ Doorbell system with camera	✓ Information Security Policy
✓ Video surveillance of entrances	✓ Work instructions for operational safety
✓ Logging of accesses to applications, specifically when entering, changing, and deleting data	✓ Work instruction access control
✓ SSH encrypted access	✓ Use of authorization concepts
✓ Certified SSL encryption	✓ Minimum number of administrators
	✓ Management of user rights by administrators
	✓ Information Security Policy

1.4. Separation Control

Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.

Technical Measures	Organizational Measures
✓ Separation of productive and test environment	✓ Information Security Policy
✓ Physical separation (systems / databases / data carriers)	✓ Work instruction operational security
✓ Multi-tenancy of relevant applications	✓ Work instruction security in software development
✓ VLAN segmentation	
✓ Client systems are logically separated	
✓ Staging of development, test, and production environment	

Pseudonymization

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

Technical Measures	Organizational Measures
✓ In case of pseudonymization: separation of the allocation data and storage in separate system (encrypted)	✓ Specific internal regulations on cryptography
✓ log files are pseudonymized at the request of the client	

2 Integrity

2.1 Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.

Technical Measures	Organizational Measures
✓ Use of VPN	✓ Information Security Policy
✓ Logging of accesses and retrievals	
✓ Provision via encrypted connections such as sftp, https and secure cloud stores	
✓ Use of signature procedures (case- dependent)	

2.2 Input Control

Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).

Technical Measures	Organizational Measures
✓ Technical logging of the entry, modification, and deletion of data	✓ Traceability of data entry, modification, and deletion through individual usernames (not user groups)
✓ Manual or automated control of the logs (according to strict internal specifications)	✓ Assignment of rights to enter, change and delete data based on an authorization concept
	✓ Information Security Policy

3 Availability and Resilience

3.1 Availability Control

Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).

Technical Measures	Organizational Measures
✓ Fire and smoke detection systems	✓ Backup concept
✓ Fire extinguisher server room	✓ No sanitary connections in the server room
✓ Server room monitoring temperature and humidity	✓ Storage of backup media in a secure location outside the server room
✓ Server room air-conditioning	✓ Separate partitions for operating systems and data where necessary
✓ UPS system and emergency diesel generators	✓ Information Security Policy
✓ Protective socket strips server room	✓ Regular testing of the diesel aggregates
✓ RAID system / hard disk mirroring	
✓ Video surveillance server room	
✓ Alarm message in case of unauthorized access to server room	

3.2 Recoverability Control

Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

Technical Measures	Organizational Measures
✓ Backup monitoring and reporting	✓ Control of the backup process ✓ Regular testing of data recovery and logging of results ✓ Storage of backup media in a safe place outside the server room ✓ Existence of an emergency plan ✓ Information Security Policy ✓ Work instruction operational security
✓ Restorability from automation tools	✓ Regular testing of data recovery and logging of results

✓ Backup concept according to criticality and customer specifications	✓ Storage of backup media in a safe place outside the server room
	✓ Information Security Policy

4 Procedures for regular Review, Assessment and Evaluation

4.1 Data Protection Management

Technical Measures	Organizational Measures
✓ Central documentation of all data protection regulations with access for employees	✓ External data protection officer appointed, DPO
✓ A review of the effectiveness of the TOMs is carried out at least annually and TOMs are updated	✓ Data Protection and Privacy Manager appointed
	✓ Regular awareness trainings at least annually
	✓ Data Protection Impact Assessment (DPIA) is carried out as required
	✓ Processes regarding information obligations according to Art 13 and 14 GDPR established
	✓ Formalized process for requests for information from data subjects is in place
	✓ Data protection aspects established as part of corporate risk management
	✓ Data Protection and Privacy Policy
	✓ Contracts and undertakings for processors and suppliers
	✓ Audits and assessment rights for processors and suppliers

4.2 Incident Response Management

Support for security breach response and data breach process.

Technical Measures	Organizational Measures
✓ Use of firewall and regular updating	✓ Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority)
✓ Use of spam filter and regular updating	✓ Formalized procedure for handling security incidents
✓ Use of virus scanner and regular updating	✓ Involvement of DPO and ISO in security incidents and data breaches

✓ Intrusion Detection System (IDS) for customer systems on order	✓ Documentation of security incidents and data breaches via ticket system
✓ Intrusion Prevention System (IPS) for customer systems on order	✓ A formal process for following up on security incidents and data breaches
	✓ Information Security Policy
	✓ Data Protection and Privacy Policy

4.3 Data Protection by Design and by Default

Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default.

Technical Measures	Organizational Measures
✓ No more personal data is collected than is necessary for the respective purpose 6	✓ Data Protection and Privacy Policy

4.4 Order Control (outsourcing, subcontractors and order processing)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

Technical Measures	Organizational Measures
✓ Monitoring of remote access by external parties, e.g. in the context of remote support	✓ Prior review of the security measures taken by the contractor and their documentation
	✓ Selection of the contractor under due diligence aspects (especially regarding data protection and data security)
	✓ Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses
	✓ Framework agreement on contractual data processing within the group of companies
	✓ Written instructions to the contractor
	✓ Obligation of the contractor's employees to maintain data secrecy
	✓ Agreement on effective control rights over the contractor
	✓ Written instructions on the use of further subcontractors
	✓ Written instructions on the destruction of data after termination of the contract
	✓ Data Protection and Privacy Policy

5 Security Measures and Compliance

Measure	GDPR compliant implemented	Comments
Physical Access Control	✓	ISO 9001 + ISO 27001
Logical Access Control	✓	ISO 27001
Authorization Control	✓	ISO 27001
Separation Control	✓	ISO 27001
Pseudonymization	✓	ISO 27001
Transfer Control	✓	ISO 27001
Input Control	✓	ISO 27001
Availability Control	✓	ISO 27001
Recoverability Control	✓	ISO 27001
Data Protection Management	✓	ISO 27001
Incident Response Management	✓	ISO 27001
Privacy by Design and by Default	✓	ISO 27001
Order Control	✓	ISO 27001
Organization	✓	ISO 9001 + ISO 27001