

Third Party Conditions for Receiving Data

These Third Party Conditions for Receiving Data (the "Third Party Conditions") govern the sharing of Data with the Designated Third Party (as defined below) by Everllence SE, Stadtbachstraße 1, 86153 Augsburg, Germany (registration number HRB22056) or Everllence Denmark, branch of Everllence SE, Teglhømsgade 41, 2450 Copenhagen SV, Denmark (registration number 31 61 17 92), or any of their Affiliates (collectively, "**Everllence**") upon specific request (the "**Request**") from a User (as defined below) .

These Third Party Conditions are supplemented by Annexes, including Annex 1 (Technical and Organisational Security Measures), Annex 2 (Compensation), and Annex 3 (Terms on Trade Secret Sharing), which form an integral part hereof. By accepting and receiving access to Data, the Designated Third Party accepts and agrees to be bound by these Third Party Conditions and the applicable annexes.

Definitions

"Affiliate" means any entity, any other entity that directly or indirectly controls, is controlled by, or is under common control with Everllence or the Designated Third Party, as applicable, where "control" means the ownership or power to vote more than fifty percent (50%) of the outstanding voting securities or other ownership interests of the entity, or the ability to otherwise direct the management and policies of the entity through ownership, by contract, or otherwise.

"Confidential Information" means any non-public information disclosed by Everllence to the Designated Third Party in connection with these Third Party Conditions or the Data, including: (a) operational data (such as sensor measurements, process values, machine parameters and system states); (b) control and configuration data (such as setpoints, limit values and calibration data); (c) performance data (such as calculated indicators, aggregated values and operating statistics); (d) alarm and event data; (e) technical documentation (such as designs, drawings, specifications, calculations, formulas, models, samples and manuals); (f) software, databases and know-how; and (g) any other technical, business or proprietary information, in any form and whether or not protected by intellectual property rights. Information need not be marked as confidential to constitute Confidential Information.

"Data" means any digital representation of acts, facts or information, and any compilation thereof, generated by the User's use of the Product and held by Everllence, which is required to be made accessible by Everllence to the Designated Third Party by a Request under applicable law.

"Data Act" means Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data, as further amended and supplemented from time to time.

"Designated Third Party" means the natural person or legal entity and/or its Affiliates designated by the User as a recipient of Data, whom must be established within the European Union.

"EULA" means the End-User License Agreement governing the User's rights to use software in and/or related to the Product from which the Data originates.

"Product" means the product or service which is provided, designed and/or manufactured by Everllence and purchased by the User, and which generates data by its use.

"Sensitive Data" means Data that contains or reveals trade secrets or other information subject to separate trade secret terms between Everllence and the Designated Third Party.

"User" means the person or legal entity that has uses the Product from which the Data originates subject to the EULA and these Third Party Conditions.

1 The Third Party's processing right

- 1.1 Subject to applicable law and these Third Party Conditions, the Designated Third Party shall process the Data made available to it pursuant to the Request strictly and only for the purposes and under the conditions agreed with the User. The Designated Third Party

shall erase Data when they are no longer necessary for the agreed purpose, or upon User's or Everllence request as set out in section 6 (Revocation of rights).

- 1.2 Everllence's obligation to provide access to Data under clause 1.1 is subject to the Designated Third Party first demonstrating, to Everllence's reasonable satisfaction, that it has implemented the technical and organisational security measures set out in Annex 1. The Designated Third Party shall provide such demonstration within a reasonable timeframe following Everllence's request. Everllence shall not unreasonably withhold or delay its confirmation. This requirement reflects the parties' acknowledgement that adequate security measures are necessary to protect the integrity and confidentiality of the Data and does not constitute an impediment to data access.
- 1.3 Everllence's obligation to provide access to Data is expressly conditioned upon (i) Everllence's acceptance of the purpose for which Data will be shared with the Designated Third Party as set out in the Request, and (ii) payment of any applicable Compensation set out in section 4 (Compensation).
- 1.4 Everllence shall have the right to withhold the Data if the Data contains technology or technical data that is subject to any national or international (re-) export control restrictions, such as but not limited to the EU Dual-Use Regulation (EU) 2021/821 or the US Export Administration Regulations (EAR, 15 CFR 730-774) if disclosing to the Designated Third Party would cause a violation of these export control restrictions.

2 Limitation of use

- 2.1 The Designated Third Party shall comply with applicable law and these Third Party Conditions. The Designated Third Party shall not, and shall ensure that its Affiliates, employees, agents and subcontractors **do not**:
 - a. disclose Data to any third party other than the User
 - b. use Data to develop a product that competes with the Product;
 - c. use Data to derive information about Everllence's business, including its production methods, operations, customers or suppliers;
 - d. use coercive means or exploit technical vulnerabilities to obtain Data;
 - e. use Data in a manner that adversely affects the security, integrity or functionality of the Product; and/or
 - f. use Data in violation of applicable law or in a manner that harms Everllence's legitimate interests.

3 Security and Privacy

- 3.1 The Designated Third Party shall implement and maintain appropriate and up to date technical and organisational measures to protect Data against unauthorised access, loss, misuse, alteration and disclosure.
- 3.2 The Designated Third Party shall comply with the specific security requirements in Annex 1.
- 3.3 If Data includes personal data, the Designated Third Party shall comply with applicable data protection law, including the GDPR. Processing of personal data on behalf of Everllence requires a data processing agreement.
- 3.4 Everllence may request documentation of the Designated Third Party's security measures.

4 Compensation

- 4.1 The Designated Third Party shall compensate Everllence for making Data available under these Third Party Conditions (the "**Compensation**"). The Compensation shall be determined by Everllence in accordance with the Data Act and on FRAND terms (fair, reasonable, and non-discriminatory).
- 4.2 Annex 2 (Compensation) sets out the terms applicable to the Compensation and contains the mandatory information explaining the basis for the calculation of the Compensation in accordance with Article 9(7) of the Data Act.

5 Confidentiality Obligations

- 5.1 The Designated Third Party shall keep Confidential Information strictly confidential and shall not disclose it to any third party without Everllence's prior written consent. The Designated Third Party shall protect Confidential Information with at least reasonable care and limit access to personnel who need to know and are bound by equivalent obligations.
- 5.2 The confidentiality obligations do not apply to information that the Designated Third Party demonstrates:
 - a. is or becomes publicly available without breach by the Designated Third Party;
 - b. was lawfully in the Designated Third Party's possession before disclosure, without confidentiality restrictions;
 - c. was received from a third party entitled to disclose it; or
 - d. was independently developed without use of Confidential Information.
- 5.3 Information is not public merely because it can be derived from public sources.
- 5.4 If legally compelled to disclose any Data or Confidential Information, the Designated Third Party shall notify Everllence promptly (to the extent permitted), cooperate in seeking protection, and disclose only the minimum required.
- 5.5 Everllence makes no representation or warranty as to the accuracy or completeness of the Confidential Information.
- 5.6 No rights in Confidential Information or related intellectual property are granted except as expressly permitted. The Designated Third Party shall not reverse engineer, decompile or create derivative works from Confidential Information or software.

6 Revocation of rights

- 6.1 The User may revoke the Designated Third Party's access to Data at any time.
- 6.2 Everllence may immediately revoke or suspend the Designated third Party's access to Data if:
 - a. any agreement between Everllence and the User (including the EULA) expires or terminates;
 - b. the Designated Third Party and/or the User breaches, or is likely to breach, these Third Party Conditions, the User Conditions or any other agreement with Everllence;
 - c. the Designated Third Party and/or the User fails to pay any amount due to Everllence within five (5) working days of a reminder;

- d. the Designated Third Party and/or the User undergoes a change of control, insolvency or similar proceedings;
 - e. continued access poses a risk to the security, integrity or confidentiality of Data.
- 6.3 Upon revocation or suspension, the Designated Third Party shall immediately cease all use of Data and, without undue delay and in any event within five (5) working days, securely delete or destroy all Data (including any copies, extracts or derivatives) in its possession or control, and provide Everllence with written certification of such deletion or destruction upon request. The Designated Third Party shall not retain any Data except to the extent required by applicable law, in which case it shall notify Everllence of such retention and continue to comply with all confidentiality and security obligations hereunder.

7 Liability and Remedies

- 7.1 The Designated Third Party is liable for any breach of these Third Party Conditions, including by its Affiliates, employees, agents, or subcontractors.
- 7.2 The Designated Third Party shall indemnify and hold harmless Everllence and its Affiliates from all claims, losses, damages, costs and expenses (including legal fees) arising from:
 - a. any breach of these Third Party Conditions;
 - b. any unauthorised use or disclosure of Data or Confidential Information; or
 - c. any third party claims arising from the Designated Third Party's use of Data.
- 7.3 The Designated Third Party shall pay the following contractual penalties:
 - a. EUR 50,000 for each breach of confidentiality (Section 4);
 - b. EUR 25,000 for each breach of the use restrictions (Section 2);
 - c. EUR 100,000 for use of Data to develop a competing product;
 - d. EUR 10,000 per day of continued breach after notice.
- 7.4 Penalties are payable within fourteen (14) days of demand, are cumulative, and do not limit other remedies.
- 7.5 The Designated Third Party's liability for breach of confidentiality, unauthorised disclosure, IP infringement or indemnification is unlimited.
- 7.6 Everllence's aggregate liability under these Third Party Conditions is limited to EUR 50,000, except as set out below.
- 7.7 Everllence is not liable for indirect, consequential or special damages, including loss of profits, revenue or business interruption.
- 7.8 Nothing in these Third Party Conditions limits Everllence's liability:
 - a. for death or personal injury caused by negligence;
 - b. for fraud, gross negligence or wilful misconduct; or
 - c. where prohibited by applicable law.

8 Injunctive relief

The Designated Third Party acknowledges that unauthorised use or disclosure of Data or Confidential Information may cause irreparable harm and that Everllence is entitled to injunctive relief and specific performance in addition to other remedies.

9 Assignment

The Designated Third Party may not assign any rights or obligations under these Third Party Conditions without Everllence's prior written consent. Everllence may assign these Third Party Conditions to an Affiliate without the Designated Third Party's consent.

10 Amendments

Everllence may amend these Third Party Conditions from time to time by providing reasonable notice to the Designated Third Party, provided that amendments shall not restrict the Designated Third Party's or the User's rights under applicable law, including the Data Act. The current version is available at <https://www.everllence.com/compliance/euda/conditions>.

11 Survival

- 11.1 The obligations of restricted use and confidentiality under Sections 2 (Limitation of use) and 5 (Confidentiality Obligations) shall survive the revocation of the Designated Third Party's access to Data and/or any Confidential Information for a period of five (5) years, except where a longer period follows from applicable law or arises from the continued retention of Confidential Information.
- 11.2 Any rights or obligations which by their nature are intended to survive the revocation of access - including but not limited to obligations regarding deletion of Data, liability and any indemnification - shall continue in full force and effect notwithstanding such revocation.

12 Law and venue

- 12.1 These Third Party Conditions are governed by Swiss law, excluding conflict of laws rules and the UN Convention on Contracts for the International Sale of Goods. Disputes shall be resolved by arbitration under ICC Rules in Zürich, Switzerland, in English, by three arbitrators. Everllence may alternatively bring proceedings in any court of competent jurisdiction.

Annex 1: Technical and Organizational Security measures to be followed by Third Party

This Annex 1: Technical and Organizational Security Measures (the "**Technical and Organisational Measures**") apply to data which may be shared to a User (as defined below) and/or a Designated Third Party (as defined below) by Everllence SE, Stadtbachstraße 1, 86153 Augsburg, Germany, company registration number HRB22056 or Everllence Denmark, branch of Everllence SE, company registration number 31 61 17 92, Tegllholmsgade 41, 2450 Copenhagen SV, Denmark as the case may be, or any Affiliate (as defined below) to said entities ("**Everllence**"). This serves as an annex to the User Conditions and/or the Third Party Conditions.

Definitions in the User Conditions and/or the Third Party Conditions shall have the same meaning in this Annex, unless expressly stated otherwise.

13 Purpose and Scope

- 13.1 This Annex sets out the minimum technical and organisational security measures required to be implemented and maintained by the User and/or the Designated Third Party, as applicable, in connection with any access to and processing of Data made available by Everllence pursuant to the Data Act.
- 13.2 The measures set out in this Annex are intended to ensure an appropriate level of security for the Data, taking into account the nature of the Data, the risks associated with unauthorised access or misuse, and the requirements set out in Articles 4(6), 5(9) and 5(10) of the Data Act.

14 General security obligations

- 14.1 The User and/or the Designated Third Party shall implement and maintain appropriate, sufficient, and up-to-date technical and organisational measures to protect the Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Data. Such measures shall:
 - a) be proportionate to the nature, scope, context and purposes of the processing of the Data; and
 - b) ensure a level of security appropriate to the risks associated with the Data.

15 Technical security measures

- 15.1 Without limitation, the following technical measures shall be implemented as a minimum:
 - a) Access control
 - Role-based access controls ensuring that access to Data is limited strictly to personnel with a demonstrable need-to-know;
 - Unique user credentials and secure authentication mechanisms;
 - Immediate revocation of access rights upon termination of employment or change of role.
 - b) Data protection and storage

Everllence

- Secure storage of Data using industry-standard encryption at rest and in transit where appropriate;
- Logical separation of Data from other datasets not covered by the relevant Request;
- Protection against unauthorised copying, extraction or bulk downloading of Data.

c) IT security and integrity

- Up-to-date malware protection, firewalls and intrusion detection or prevention mechanisms;
- Regular security updates and patch management;
- Measures to ensure the integrity and availability of Data and systems used to process the Data.

1.1.a.2 Logging and Monitoring

- Centralized logging of access, downloads, configuration changes, and administrative actions.
- Maintain logs at least as long as required for legal/contractual obligations and for incident investigation.

16 Organisational security measures

a. Internal governance and policies

- Adopt and maintain internal policies governing access to, use of and protection of Data;
- Ensure that personnel with access to Data are subject to appropriate confidentiality obligations.

b. Training and awareness

- Ensure that relevant personnel receive appropriate training on data security, confidentiality and applicable legal obligations.;

c. Incident management

- Maintain procedures for identifying, managing and responding to security incidents affecting the Data;
- Promptly notify Everllence without undue delay (within 72 hours) of any actual or suspected unauthorised access, use or disclosure of Data.

17 Monitoring, audit and documentation

17.1 Everllence may, acting reasonably, request information and documentation demonstrating compliance with this Annex, including descriptions of the technical and organisational measures implemented.

17.2 Failure to demonstrate compliance may result in suspension or revocation of access to Data in accordance with the applicable Conditions for Receiving Data.

Annex 2 Compensation to the Third party Conditions for receiving Data

These Terms on Compensation (the "**Compensation Terms**") apply to data sharing with a Designated Third Party by Everllence SE, Stadtbachstraße 1, 86153 Augsburg, Germany, company registration number HRB22056 or Everllence Denmark, branch of Everllence SE, company registration number 31 61 17 92, Teglholmsgade 41, 2450 Copenhagen SV, Denmark , or any Affiliate ("**Everllence**"), upon request (the "**Request**") from a User under Regulation (EU) 2023/2854 (the "**Data Act**").

These Compensation Terms supplement the Third Party Conditions, which remain fully applicable. In case of conflict, these Compensation Terms prevail.

"Affiliate" means any entity, any other entity that directly or indirectly controls, is controlled by, or is under common control with Everllence or the Designated Third Party, as applicable, where "control" means the ownership or power to vote more than fifty percent (50%) of the outstanding voting securities or other ownership interests of the entity, or the ability to otherwise direct the management and policies of the entity through ownership, by contract, or otherwise.

"Data" means data held by Everllence originating from the User's use of the Product, to be shared with the Designated Third Party upon a Request.

"Designated Third Party" means the person or entity (including Affiliates) designated by the User as recipient of Data under a Request, established within the European Union.

"Product" means the product identified in a Request, designed or manufactured by Everllence and purchased by the User, which generates data through use.

"Third Party Conditions" means the conditions governing Everllence's sharing of Data with the Designated Third Party.

"User" means the person or entity that has entered into an End-User License Agreement with Everllence for the Product.

Amount of compensation

Based on the cost calculation prepared by Everllence in accordance with the principles set out below, Everllence charges the following Compensation:

One-time Compensation: EUR [●]

Annual recurring Compensation: EUR [●]

To be paid as of [DATE]: EUR [●]

18 Basis and general principles

- 18.1 The Designated Third Party shall pay Everllence for making Data available pursuant to a Request (the “**Compensation**”).
- 18.2 Everllence determines and charges the Compensation on fair, reasonable and non-discriminatory (FRAND) terms.
- 18.3 Everllence structures the Compensation to reflect only such costs and investments as are appropriate and justified, including:
- a. direct and incremental costs of making the Data available following a Request; and
 - b. where applicable, a proportionate share of investments to enable secure third-party data access.
- 18.4 Everllence will provide information on how the Compensation was calculated in sufficient detail for the Designated Third Party to understand the basis.

19 Structure of the compensation

- 19.1 The Compensation consists of:
- a. One-time costs per Request, including:
 - authorisation and compliance checks for the Request;
 - technical onboarding and configuration for the Designated Third Party; and
 - a pro rata share of development costs to adapt Everllence’s systems for third-party access.
 - b. Annual recurring costs per Request, including:
 - ongoing maintenance of third-party access functionalities; and
 - connectivity support and troubleshooting for the Designated Third Party’s access.
- 19.2 The Compensation may include a reasonable, objectively justified and non-discriminatory margin.

20 Pro rata development costs

- 20.1 Pro rata development costs reflect investments by Everllence to enable third-party data access, including:
- a. development and adaptation of technical architecture for external access;
 - b. access control, authentication, monitoring and security measures for third-party access; and
 - c. governance, documentation and compliance frameworks for third-party data sharing.
- 20.2 General development costs for the Product or Everllence’s platforms are not included in the pro rata development costs.

Everllence

21 SMEs and not-for-profit research organisations

- 21.1 If the Designated Third Party is an SME or not-for-profit research organisation, the Compensation is limited to pro rata costs with no margin.

22 Review and adjustment

- 22.1 Everllence may review and adjust the Compensation to reflect changes in:
- a. underlying costs;
 - b. the expected volume of third-party data sharing requests;
 - c. applicable law or regulatory guidance.
- 22.2 Adjustments will be notified in advance and apply only to Annual Recurring Compensation and future Requests.