



Personal Data Processing Clauses

The following terms and conditions are an integral part of the Eaton Purchase Order Terms and Conditions ("PO T&Cs") and, where applicable, acceptance of the PO T&Cs is also acceptance of these terms and conditions.

For the purpose of this set of clauses:

- Processor means the Service Provider or Seller (as applicable)
- Controller means Eaton or the Buyer (as applicable)
- Personal Data means any information relating to an identified or identified natural person ('data subject'),

1. Instructions

Processor may process Personal Data only on documented instructions from Controller (including data transfers abroad unless legally required to transfer and in which case Processor will inform Controller of the legal requirement before processing personal data unless that law prohibits this on important grounds of public interest).

Processor shall immediately inform Controller if in its opinion an instruction breaches any applicable data protection law.

If Processor determines purpose and means of processing in breach of any applicable data protection law, Processor will be considered a Controller.

2. Records of processing Activities

Processor must keep records of its processing activities performed on behalf of the Controller, including

- name and contact details of the Processor, Controller, and respective data processing officer if applicable;
- categories of processing carried out on behalf of each controller;
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards; a description of the technical and organizational security measures.

3. Sub-processing

Sub-processing shall be authorized in advance by Controller through either a general or a specific written authorization. Where Personal Data is processed by sub-contractors the Processor shall:

- not authorize any third party and/or sub-contractor to process the Personal Data ("sub-processor") other than with the prior written consent of the Controller and:
- remain fully liable to the Controller for any failure by a sub-processor to fulfil its obligations in relation to the processing of any Personal Data; and the use of any sub-processor being otherwise in accordance with this clause.

The Controller has the right at any time to demand from Processor full details of the processing to be undertaken by the proposed sub-processor and a copy of the contract between the Processor and the sub-processor.

The Processor must ensure that the contract between Processor and sub-processor includes the same terms as those set out in these clauses. In cases of transfer of Personal Data outside the European Economic Area, the contracts shall incorporate a legal mechanism to ensure an adequate level of protection of the Personal Data transferred.

In case the Controller grants a general authorization to sub-processing Personal Data, the Processor shall inform the Controller of any intended changed concerning the addition or replacement of sub-processors, giving the Controller the opportunity to object.

4. Confidentiality

Where Personal Data is processed by the Processor, its agents, sub-contractors or employees, the Processor shall, and shall procure that its agents, sub-contractors and employees to:

- take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Personal Data, as strictly necessary to perform the Services in the context of that individual's duties to the Processor, ensuring that all such individuals;
- are informed of the confidential nature of the Personal Data;
- have undertaken appropriate training in relation to Personal Data Protection;
- are subject to confidentiality undertakings or professional or statutory obligations of confidentiality;
- are aware of the Processor 's obligations in relation to data protection under these clauses; and
- keep all Personal Data and any analyses, profiles or documents derived there from separate from all other data and documentation of the Processor.

5. Security

Where Personal Data is processed by the Processor, its agents, sub-contractors or employees, the Processor shall:

- implement and ensure that its agents, sub-contractors and employees implement appropriate technical and organizational security measures to ensure a level of security commensurate with the risks associated with the processing, such measures to be appropriate in particular to protect against accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to the Personal Data. These measures shall take into account and be appropriate to the state of the art, nature, scope, context and purposes of processing and risk harm which might result from unauthorized or unlawful processing or accidental loss, destruction or damage to Personal Data and may include (as appropriate):
- as appropriate pseudonymising or encrypting Personal Data;
- ensuring the on-going confidentiality, integrity and, availability of processing systems and services;
- ensuring a means to restore the availability of and access to Personal Data in a timely manner following any physical or technical incident; and
- having in place a process for regularly testing, assessing and evaluating the effectiveness of the technical and organizational security measures.

6. Data Subjects Rights

Processor shall assist Controller with requests to exercise Data Subject rights, including but not limited to the right to access and the right to erasure.

7. Personal Data Breach

Where Personal Data is processed by the Processor, its agents, sub-contractors or employees, the Processor shall, and shall procure that its agents, sub-contractors and employees to inform the Controller without undue delay and in any case no later than 24 hours upon becoming aware of a Personal Data Breach by sending an email to DataProtection@Eaton.com describing the Personal Data Breach in terms of who and how many data subjects are affected, where, when and how it occurred, which measures have been taken already to stop the breach and mitigate its effects. Upon Controller's request, Processor shall cooperate with the Controller without delays and provide all available information to Controller to support the data breach investigation and notification to the relevant data protection authority/ies and/or data subjects..

8. Data Protection Impact Assessments

Taking into account the nature of processing and information available to Processor, Processor shall assist Controller in cases a Data Protection Impact Assessment shall be carried out.

9. Cooperation with Data Protection Authorities

Processor are required to cooperate, on request with Data Protection Authorities in the performance of their tasks.

10. Availability of Information

Upon written request of the Controller, the Processor will undertake its commercially reasonable efforts to make available to the Controller reasonable information necessary to demonstrate compliance with its obligations regarding data protection as explicitly set out in these clauses or by applicable law and allow for and contribute to audits, including inspections, conducted by the Processor or another auditor mandated by the Processor.

11. Deletion of Existing Personal Data

Where Personal Data is processed by the Processor, its agents, sub-contractors or employees, the Processor shall, and shall procure that its agents, sub-contractors and employees to:

- ensure that any IT systems used in the context of performance of these clauses, including any backup systems, allow the erasure or deletion of specific Personal Data, and put in place measures to fully implement any erasure or deletion request within the timeframe required by Controller;
- upon termination for any reason of the provision of Services, cease processing the Personal Data immediately, except for the safe storing. Thereafter, at the Controller's option, either return, or delete from its systems (so that such Personal Data cannot be recovered or reconstructed), the Personal Data and any copies of it or of the information it contains, including any Personal Data in hardcopy format and the Processor shall confirm in writing to the Controller that this clause has been complied with in full.
