

Appendix 2 Data Processing Addendum (DPA)

This Data Processing Agreement (hereinafter: "DPA") has been drawn up in accordance with Regulation (EU) 2016/679 (GDPR), in particular Article 28 paragraphs 3 and 4, and forms an integral part of the Agreement for the use of the ICEWORX Platform.

Section I – General Provisions

Article 1 – Purpose and scope

- a) The purpose of this DPA is to ensure compliance with Article 28 (3) and (4) of the GDPR with regard to the processing of Personal Data by ICEWORX as a Processor on behalf of the Client as a Controller;
- b) This DPA applies to the processing of Personal Data as specified in **Annex I**;
- c) *Annexes I and II* form an integral part of this DPA;
- d) This DPA is without prejudice to the obligations to which the Controller is subject under the GDPR;
- e) This DPA does not, by itself, ensure compliance with international transfer requirements set out in Chapter V GDPR.

Article 2 – Immutability

1. The parties undertake not to amend this DPA, other than to supplement or update the Annexes.
2. This does not prevent Parties from incorporating the DPA into a broader agreement or adding additional provisions, provided that it does not conflict with the GDPR or the rights of data subjects.

Article 3 – Hierarchy

In the event of any conflict between this DPA and any provision of the other Annexes or the Agreement, this DPA shall prevail as far as the processing of Personal Data is concerned.

Section II – Obligations of the Parties

Article 4 – Instructions

1. The Processor shall only process Personal Data on the basis of documented instructions from the Controller, unless Union or national law requires processing. In such case, the Processor shall inform the Controller prior to the processing, unless prohibited by law.
2. The Processor shall inform the Controller without undue delay if it considers that an instruction violates the GDPR or other applicable privacy laws.
3. The Controller guarantees that it is entitled to give the Processor the instructions provided and that their execution is not in violation of the GDPR.

Article 5 – Purpose limitation and retention period

1. The Processor shall only process Personal Data for the specific purposes described in **Annex I**, unless it receives further instructions from the Controller.
2. The processing will only take place during the period specified in Annex I.

Article 6 – Security

1. The Processor shall implement and maintain appropriate technical and organizational measures for the security of Personal Data, as described in **Annex II**. These measures are designed to protect data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.
2. When determining appropriate security measures, the Processor takes into account the state of the art, the implementation costs, the nature, scope, context and purposes of the processing, as well as the risks for data subjects.
3. The Processor shall only grant access to Personal Data to employees for whom access is strictly necessary for the performance of the agreement. The Processor shall ensure adequate confidentiality obligations for all employees involved.

Article 7 – Sub-processors

1. The Processor uses Sub-processors. When engaging Sub-processors, the Processor imposes on the Sub-processor the same data protection obligations as included in this DPA, in particular with regard to sufficient guarantees regarding technical and organizational security measures.
2. The Processor remains fully liable to the Controller for the fulfilment of obligations by Sub-processors.
3. The Processor shall inform the Controller in writing and at least thirty (30) days prior to any intended changes to the list of Sub-processors. The Data Controller has the right to object to an intended change. The current list of Sub-processors is available upon request.

Article 8 – Rights of data subjects

1. The Processor shall assist the Controller, to the extent technically and organisationally possible, in the fulfilment of its obligations with regard to requests from data subjects under the GDPR, including the right of access, rectification, erasure, restriction of processing, portability and objection.

2. The Processor shall forward requests from data subjects submitted directly to it to the Controller without undue delay.

Article 9 – Privacy by design and privacy impact

The Processor shall assist the Controller, in view of the nature of the processing and the available information, with:

- a. complying with the obligation to carry out a data protection impact assessment (DPIA) if required;
- b. prior consultation with the supervisory authority if a DPIA indicates that the processing would pose a high risk that cannot be mitigated.

Article 10 – Documentation and audit

1. The Processor shall make available to the Controller all information that is reasonably necessary to demonstrate compliance with the obligations under this DPA.
2. At the request of the Controller, the Processor shall permit audits, including inspections, carried out by the Controller or an independent auditor mandated by it, with reasonable notice and no more than once every twelve (12) months, unless there are demonstrable indications of non-compliance.
3. The costs of an audit shall be borne by the Controller, unless the audit shows demonstrable non-compliance by the Processor.

Article 11 – Data breaches

1. The Processor shall report a Data Breach to the Controller without undue delay, at the latest within 36 hours after the Processor has become aware of it. The notification must contain at least:
 - a. a description of the nature of the Data Breach, including, where possible, the categories and the estimated number of individuals and data records involved;
 - b. the contact details of the Data Protection Officer or other contact point for further information;
 - c. the likely consequences of the Data Breach;
 - d. the measures taken or proposed to remedy the Data Breach and limit the negative consequences.
2. If not all information is immediately available, the Processor shall provide the available information as soon as possible and supplement it in phases.
3. The Processor shall assist the Controller in the fulfilment of its notification obligations towards the Dutch Data Protection Authority (or other competent supervisory authority) and data subjects pursuant to Articles 33 and 34 of the GDPR.

Section III – Final provisions

Article 12 – Non-compliance and termination

1. If the Processor breaches its obligations under this DPA, the Controller may instruct the Processor to cease processing until compliance is restored.
2. The Controller has the right to terminate the processing activities if: (i) the processing has been suspended for more than one month without redress of compliance; (ii) the Processor is in material or systematic breach of the DPA or the GDPR; or (iii) the Processor fails to comply with a binding decision of a competent court or supervisory authority.
3. Upon termination, the Processor shall, at the option of the Controller, destroy or return all Personal Data processed on its behalf and confirm this in writing, unless Union or national law requires retention.

Article 13 – Applicable law

Dutch law applies to this DPA. Disputes are submitted to the competent court in Rotterdam, without prejudice to the right of data subjects to turn to the Dutch Data Protection Authority.

Annex I – Description of the Processing

Categories of data subjects

- Users: employees of the Data Controller who use the Platform.
- End Recipients: customers of the Data Controller whose address and contact details are processed for the purpose of the shipment.

Categories of Personal Data

- Users: first name, last name, email address, telephone number, IBAN and other data entered for the purpose of providing services or support.
- Final recipients: (initials,) first name, last name, address, e-mail address, telephone number and other data required for the shipping service.

Special categories of personal data

No special categories of Personal Data as referred to in Article 9 of the GDPR are processed.

Nature and purposes of the processing

- Users: identification for access to the Platform; providing customer support.

- End Recipients: processing of shipment order data required for the execution of transport orders by Carriers and for track & trace functionality.

Retention periods

Personal data will not be stored longer than necessary for the purposes described above: User account data: will be deleted within 90 days after termination of the Agreement, unless legal retention obligations require a longer period. End Recipients' shipping order data will be retained for the duration of the Agreement and the legally required retention period for the Controller's administration. After the retention period has expired, Personal Data will be deleted or anonymized in such a way that it can no longer be traced back to individual data subjects.

Annex III – Technical and organisational measures

ICEWORX is constantly evaluating and improving its security measures. The key measures include:

- Encryption of data at rest at the storage level and in transit (TLS 1.2 or higher);
- Hosting on a dedicated server capacity in the Iron Mountain AMS-1 data center in Haarlem
- The Iron Mountain AMS-1 data center in Haarlem is one of the most extensively certified data centers in The Netherlands:
 - ISO 27001 (Information Security)
 - ISO 22301 (Business Continuity)
 - ISO 9001 (Quality Management)
 - ISO 14001 (Environmental Management)
 - ISO 50001 (energy management)
 - PCI DSS
 - SOC 2 Type I en Type II
 - Tier 3 rating

The physical infrastructure, power supply, cooling, physical access security and business continuity are therefore subject to a heavily certified regime.