



DPA

This Data Processing Agreement (DPA) is incorporated into the Agreement between Qargo and Customer. It outlines Qargo's obligations as a Processor of Customers' Personal Data.

The DPA's purpose is to ensure such processing is conducted in accordance with Data Protection Laws and respects the Customer's rights where the Customer's Personal Data is processed under the Agreement.

1. Definitions

Capitalised terms not defined in this DPA can be found in the MSA. Capitalised terms in this DPA shall have the following meaning:

"Data Controller" means the entity that determines the purposes and means of the Processing of Personal Data, as defined in the Data Protection Laws;

"Data Processor" means the entity which Processes Personal Data on behalf of the Data Controller, as defined in the Data Protection Laws;

"Data Protection Laws" means all data protection and privacy laws, including guidance issued by any data protection authority, applicable to any Personal Data, as may be amended or replaced from time to time, including without limitation:

- a. in the UK, the Data Protection Act 2018, the United Kingdom General Data Protection Regulation (UK GDPR), and any legislation implemented in connection with these legislations.
- b. in the European Union, it also includes the EU General Data Protection Regulations (EU GDPR), including any replacement legislation coming into force from time to time.
- c. in the United States of America, it also includes the California Consumer Privacy Act, as amended.

"Data Subject" means the individual to whom Personal Data relates, as defined in the Data Protection Laws;

"GDPR Laws" means the EU GDPR and the UK GDPR collectively.

"Customer Personal Data" means data about a natural person processed by the Data Processor on behalf of the Data Controller in relation to the provision of the Services under the Agreement, from which that person is identified or identifiable, as defined in the Data Protection Laws .

"Personal Data" has the meaning given to it in the GDPR Laws.

"Personal Data Breach" means any breach of security or other action or inaction leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data processed by Qargo under this DPA by Qargo, its Sub-processors or any other identified or unidentified third party.

"Sub-processor" means any third party engaged by Qargo to Process Personal Data on behalf of the Controller in connection with the Services;

"Supervisory Authority" means the ICO, or any other competent data protection or supervisory authority with jurisdiction over the Processing of Personal Data under this DPA;



2. Roles of the Parties

- 2.1. **Processing Personal Data.** The Parties accept and agree that the Services shall include processing of Personal Data.
- 2.2. **Roles.** In respect of Customer Personal Data processed by Qargo on the Customer's behalf as part of the Services, the Parties acknowledge that Qargo shall act as Data Processor and the Customer shall act as Data Controller of such Customer Personal Data.
- 2.3. **Processing particulars.** The duration of the processing, nature, purpose, as well as types of Personal Data and categories of Data Subjects processed under this DPA are specified in the table in clause 3.2.
- 2.4. **Compliance.** Both Parties will comply with all applicable requirements of the Data Protection Laws in exercising its rights and performing its obligations under this Agreement, as such laws apply to a Controller and Processor respectively.
- 2.5. **Controller responsibility.** The Customer, as Data Controller, determines the purposes and means of processing Customer Personal Data through the Services. Where the Customer enables the collection of driver location, telematics or other monitoring of individuals through the Services (including via the Driver App), the Customer is responsible for (a) establishing and documenting a lawful basis for that processing; (b) providing all notices and transparency information required to the relevant Data Subjects; and (c) determining whether a data protection impact assessment is required under Article 35 of the GDPR (or equivalent provisions of the Data Protection Laws) and, where required, carrying it out. Qargo processes such Personal Data solely as a Processor on the Customer's Documented Instructions and will provide reasonable assistance in accordance with this DPA.

3. Data Processing

- 3.1. **Scope and Rules.** This DPA applies when Qargo processes Customer Personal Data under the Agreement.
- 3.2. **Details of the Processing.**

Subject matter	The subject matter of the data processing under this DPA is Customer Personal Data.
Duration	Customer Personal Data shall be processed under this DPA for as long as necessary to provide the Services as described in the Agreement, as legally or contractually required, or upon receipt of Customer's written request for deletion
Nature and purpose	Qargo will process the Customer Personal Data for the purpose of providing the Services to the Customer in accordance with the Agreement.
The frequency of the transfer	Continuous with use of the Services.
Categories of Data Subject	The categories of Data Subject, whose Personal Data may be processed by Qargo as part of Customer Data include (but are not limited to) Customer's clients and prospects; Customer's officers and directors; Customer's employees, temporary workers, agents, drivers and volunteers; independent contractors engaged by the Customer; Customer's suppliers and vendors; advisors,

	consultants and other professional experts engaged by the Customer; and any other categories of Personal Data that may be contained in the Customer Data provided to the Data Processor in accordance with the Agreement.
Categories of Personal Data	The categories of personal data transferred are determined solely by the Data Controller. In the normal course of the Data Processor's service, the categories of Personal Data transferred might include (but are not limited to): contact details (name, email address, telephone number); job titles and roles; vehicle and driver information; location data relating to transport jobs; operational data relating to transport jobs; financial data (where relevant to invoicing); and any other Personal Data uploaded by the Customer to the Services.
Special Category Data	Special category data (as defined in the Data Protection Laws) is not anticipated to be processed in the normal course of the Services. Customer shall not share any Special Category Data with Qargo without agreeing additional safeguards in advance.

4. Instructions

- 4.1. **Documented Instructions.** The Parties agree that this DPA and the Agreement (including any instructions provided by the Customer to Qargo required for or in relation to the Services) constitute Customer's documented instructions regarding Qargo's processing of Customer Personal Data ("Documented Instructions").
- 4.2. **Processing on instruction.** Qargo will only process the Customer Personal Data in accordance with Documented Instructions, including instructions regarding the transfer of Customer Personal Data to a third country or an international organisation, unless otherwise required by applicable law, in which case Qargo will, to the extent permitted, inform the Customer of that legal requirement before processing. Qargo shall promptly inform Customer if, in Qargo's opinion, an instruction from Customer infringes the Data Protection Laws.
- 4.3. **Instructions outside scope.** If Documented Instructions provided by Customer require Qargo to perform actions that go beyond its obligations under this DPA or the scope of work for the Services set out in this Agreement or an instruction given by the Customer breaches the Data Protection Laws, Qargo shall inform the Customer and require the Customer to provide different Documented Instructions, the carrying out of which fall within the scope of the Services or within Qargo's obligations under this DPA.

5. Confidentiality

- 5.1. **Confidentiality of personnel.** Qargo will take reasonable steps to ensure the reliability of any persons authorised to process any Customer Personal Data (including employees, agents, and contractors) and shall ensure that all such persons are subject to a binding obligation of confidentiality in respect of such Personal Data, whether by contract or by operation of law, such obligation survives the termination of that person's employment or engagement with Qargo.

6. Security

- 6.1. **Technical and organisational measures.** Considering the nature, scope, context and purpose of processing, Qargo will maintain appropriate technical and organisational



QARGO

measures to protect the Customer against unauthorised or unlawful processing of Customer Personal Data and against accidental loss, destruction or alteration to, such Customer Personal Data, taking into account the nature of the Personal Data in accordance with Article 32 of the GDPR (or equivalent provisions of the Data Protection Laws). Further detail on the technical and organisational measures maintained by Qargo is available at <https://trust.qargo.com>, as updated by Qargo from time to time.

- 6.2. **Adequacy of measures.** The Parties agree that for the purposes of processing Customer Personal Data under this DPA and the Agreement, the measures contained within relevant security measures available at <https://trust.qargo.com> are appropriate, given the nature of the data to be processed and the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction, disclosure, access or damage.
- 6.3. **Security certification.** Qargo's Information Security Management System (ISMS) governing the Services is certified compliant with the ISO/IEC 27001:2022 standard and Qargo will continue to maintain such certification (or equivalent) for the duration of the Subscription Period.

7. Sub-processing

- 7.1. **List of Sub-processors.** A list of Qargo's Sub-processors is available at <https://trust.qargo.com/>.
- 7.2. **General authorisation.** The Customer consents to Qargo using sub-processors for processing Personal Data under this Agreement. The Customer also provides general authorization for Qargo to replace or add sub-processors.
- 7.3. **Sub-processor obligations.** Qargo will ensure that any sub-processor is engaged through a written agreement with data processing commitments no less stringent than those in this Agreement, including obligations of confidentiality and data security no less protective than those set out in this Agreement, and binding the sub-processor to keep the Personal Data confidential and to use it only for the purposes of providing the relevant part of the Services. Qargo remains liable to the Customer for the actions of its sub-processors.
- 7.4. **Changes to Sub-processors.** Qargo must inform the Customer in line with section 11 of the MSA of any intended changes regarding the addition or replacement of sub-processors, giving the Customer an opportunity to reasonably object. If no objection is raised within thirty (30) days, the changes are considered accepted. If an objection is raised and no agreement is reached within thirty (30) days, Qargo may proceed with the change, and the Customer has the right to terminate the Agreement.

8. Cross-Border Transfers

- 8.1. **Restrictions on transfers.** The Customer's authorisation of Qargo's sub-processors under clause 7.2 constitutes the Customer's prior authorisation for the transfer of Customer Personal Data to those sub-processors, including where located outside the UK, the EU or a country subject to an adequacy decision. Qargo will ensure any such transfer is subject to an appropriate transfer mechanism in accordance with clause 8.2.
- 8.2. **Transfer mechanisms.** Where Qargo engages a sub-processor to process Personal Data outside the UK, the EU, or a country subject to an adequacy decision (a) and such data originates in the EU, Qargo shall ensure that such transfer is subject to the EU Standard Contractual Clauses (Module 3: Processor to Processor), or another valid transfer mechanism recognised under Data Protection Laws, and (b) where such data originates in the UK, Qargo shall ensure that the Information Commissioner's Office of the United Kingdom's International Data Transfer Addendum will apply.
- 8.3. **Sub-processor audit evidence.** Qargo will require, in the written agreement referred to above, that the Sub-processor permits Qargo to audit, or obtain audit reports or



QARGO

equivalent evidence regarding, the Sub-processor's compliance with its data protection obligations; and Qargo shall, upon the Controller's reasonable request, make available to the Controller a summary of relevant Sub-processor certifications or audit reports (such as ISO 27001 or SOC 2 reports) to the extent Qargo holds them.

- 8.4. **Changes to UK transfer safeguards.** The Parties agree that Qargo, may at its sole discretion, update, and or entirely replace paragraphs which concern Customer Data which originates from the UK being transferred outside of the UK, the EU, or a country subject to an adequacy decision, if the Information Commissioner's Office provides an alternative or replacement recognised compliance standard for such transfers in accordance with the UK GDPR, to that already stated in the DPA. Qargo will provide notice of such change to the Customer.

9. Data Subject Requests and Assistance

- 9.1. **Notification of requests.** Qargo shall use reasonable efforts to promptly notify the Customer if:
- 9.1.1. it receives a request from a Data Subject under any Data Protection Laws in respect of Personal Data and shall not respond to that request directly without the Controller's prior written consent, except to confirm receipt of the request or as required by applicable law;
 - 9.1.2. a complaint or request relating to Customer's obligations under the Data Protection Laws; or
 - 9.1.3. any other communication relating directly or indirectly to the processing of any Personal Data in connection with the Agreement.
- 9.2. **Assistance to the Controller.** Considering the nature of processing and the information available to Qargo, Qargo will use reasonable efforts to:
- 9.2.1. provide the Controller with reasonable assistance, insofar as this is possible taking into account the nature of the Processing, to enable the Controller to respond to requests from Data Subjects exercising their rights under Data Protection Laws;
 - 9.2.2. Assist Customer in responding to requests or demands made to Customer by any court or governmental authority responsible for enforcing the Data Protection Laws;
 - 9.2.3. maintain accurate written records of all categories of Processing activities carried out on behalf of the Controller under this Agreement, in accordance with Article 30(2) of the GDPR (or equivalent provisions of the Data Protection Laws), and make such records available to the Controller upon reasonable request; and
 - 9.2.4. provide the Controller with reasonable assistance with any data protection impact assessments, and with any prior consultations with a Supervisory Authority, which the Controller reasonably considers to be required by Article 35 or 36 of the GDPR (or equivalent provisions of the Data Protection Laws), taking into account the nature of the Processing and information available to Qargo;

10. Deletion or return of Data

- 10.1. **Deletion or return.** On termination or expiry of the Agreement, and subject to (a) the Customer's right to request an export of Customer Data under clause 2.9 of the MSA and (b) where it applies, the EU Data Act Addendum, Qargo shall, at the Customer's choice, return or delete all Customer Personal Data and delete existing copies, unless Qargo is required by applicable law to retain a copy. Qargo shall, upon the Customer's written request, confirm in writing that such deletion or return has been completed



11. Breach identification and notification

- 11.1. **Notification and assistance.** Processor shall notify the Customer of any Personal Data Breach of which it is aware without undue delay, but in any event within 72 hours, and shall provide the Customer with reasonable assistance in responding to a Personal Data Breach. Such assistance shall include providing the Customer with the information reasonably necessary to comply with its obligations under Articles 33 and 34 of the GDPR (or equivalent provisions of the Data Protection Laws), including (to the extent available to Qargo) the categories and approximate number of Data Subjects and personal data records concerned, the likely consequences of the breach, and the measures taken or proposed to address it and mitigate its possible adverse effects.

12. Access & Audit

- 12.1. **Audit rights.** Upon request, Qargo shall allow the Controller, the ICO, the national authority of the Controller and its representatives access to Qargo's premises, records and personnel for the purposes of assessing Qargo's compliance with its obligations under this Agreement.
- 12.2. **Audit conditions and limits.** Save where access is required by the ICO or another Supervisory Authority, Qargo shall not be required to provide the Controller with access to its premises, records or personnel under this clause more than once in any 12-month period, and any such access by the Controller shall: (i) only be exercised where the Controller reasonably believes a Personal Data Breach affecting the Controller's Personal Data has occurred, or a Supervisory Authority has required an audit; (ii) otherwise be satisfied by Qargo providing available third-party certifications (such as ISO 27001 or SOC 2 reports), completed security questionnaires, and other documentation reasonably demonstrating compliance; (iii) be conducted on no less than 30 days' prior written notice, during normal business hours, and in a manner that does not unreasonably disrupt Qargo's business; and (iv) be at the Controller's own cost, unless the audit identifies a material breach of this DPA by Qargo, in which case Qargo shall reimburse the Controller's reasonable costs of that audit.
- 12.3. **Information on request.** Upon request, Qargo shall provide the Customer with information necessary to demonstrate the Customer's compliance with obligations under Data Protection Laws and this DPA.

DPA Attachment 1: US State Privacy Addendum

This Addendum supplements the Data Processing Agreement and applies where Qargo Processes Personal Information (as defined in the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (the "CCPA")) on the Customer's behalf. Where US state privacy law applies to such Personal Information, this Addendum controls over any conflicting term of the DPA, and the definition of "Data Protection Laws" is deemed to include the CCPA and other applicable US state privacy laws.

For the purposes of the CCPA, the Customer is the "business" and Qargo is a "service provider". Qargo will: (a) Process Personal Information only for the specific business purpose(s) set out in the Agreement and not for any other purpose; (b) not sell or share Personal Information (as "sell" and "share" are defined in the CCPA); (c) not retain, use or disclose Personal Information outside the direct business relationship with the Customer, or for any purpose other than the services specified in the Agreement, except as permitted by the CCPA; (d) not combine Personal Information with personal information received from, or on behalf of, any third party, or collected from Qargo's own interactions, except as permitted by the CCPA; (e) provide the same level of privacy protection as is required of a business under the CCPA; (f) notify the



Customer without undue delay if it determines that it can no longer meet its obligations under the CCPA; and (g) grant the Customer the right, on notice, to take reasonable and appropriate steps to stop and remediate unauthorised use of Personal Information.

Qargo certifies that it understands the restrictions in this Addendum and will comply with them. The Customer may, on reasonable notice, take reasonable and appropriate steps to help ensure that Qargo uses Personal Information transferred under the Agreement in a manner consistent with the Customer's obligations under the CCPA.