

Data Processing Agreement

Go4Future Consulting e.U. – DeCA Portal

Version: 1 October 2026

Preamble

This Data Processing Agreement (hereinafter the "DPA") is concluded between the customer, as identified by the company data provided upon registration (hereinafter the "Controller") and Go4Future Consulting e.U., Dr. Rudolf Klafsky-Straße 18, 2500 Baden, Austria, Company Register No. FN 684502x (Regional Court Landesgericht Wiener Neustadt), VAT ID No. ATU83497057 (hereinafter the "Processor" or "G4F").

The Controller uses the DeCA Portal platform on the basis of the General Terms and Conditions and the Terms of Use (hereinafter jointly the "Main Agreement"). In doing so, G4F processes personal data on behalf of the Controller. This DPA governs the rights and obligations of the parties pursuant to Article 28 GDPR. It forms an integral part of the Main Agreement.

The DPA is concluded in electronic form as part of the registration process. It thereby satisfies the formal requirement of Article 28(9) GDPR. G4F logs the time, the consenting user account and the version of the text accepted, and makes the version in force from time to time as well as all earlier versions permanently available to the Controller for retrieval in the customer account.

1. Subject Matter, Nature and Purpose of the Processing

1.1 The subject matter of the processing on behalf of the Controller is the provision of the services described in the Main Agreement, insofar as personal data for which the Controller is responsible are processed in the course of doing so.

1.2 The nature, purpose and scope of the processing, the categories of data subjects and the types of personal data are specified in Annex 1.

1.3 Processing takes place exclusively in Member States of the European Union or in states party to the Agreement on the European Economic Area, unless otherwise provided in clause 8.

1.4 This DPA does not cover processing operations that G4F carries out as controller in its own right, in particular the administration of the contractual relationship, invoicing, system security and the use of anonymised and aggregated data. Information on these is provided in G4F's Privacy Policy.

2. Duration

2.1 This DPA commences upon the conclusion of the Main Agreement and ends upon its termination.

2.2 Beyond the end of the Main Agreement, the provisions of this DPA continue to apply for as long as G4F holds personal data of the Controller in storage, in particular during the post-termination periods set out in clause 12.

3. The Controller's Right to Issue Instructions

3.1 G4F processes personal data exclusively on the documented instructions of the Controller. This also applies to the transfer of personal data to a third country, unless G4F is required to do so by Union or Member State law to which G4F is subject; in such a case, G4F shall inform the Controller of that legal requirement

before processing, unless that law prohibits such information on important grounds of public interest.

3.2 The Main Agreement, including the Terms of Use, as well as the settings and entries made by the Controller via the functions of the Platform, shall be deemed to constitute documented instructions.

3.3 The following in particular shall be deemed express instructions of the Controller:

- the storage of the electronic control documents uploaded by the Controller or generated in the Platform from the particulars entered by the Controller or by Drivers acting for it, the generation of an Issued Copy, preceded by a Cover Page where a document has been uploaded, and the making available of such copies, including the assignment to each document of a unique web address that can be retrieved without any additional log-in, as required by the applicable provisions governing road haulage;
- the provision of documents and notifications to Drivers and to third parties designated by the Controller;
- the retention of the generated documents for the periods specified in clause 12.

3.4 The Controller acknowledges that public retrievability pursuant to clause 3.3(a) is a requirement of the applicable legal provisions and that the data are thereby accessible to any person who has the address or the associated QR code. G4F applies the risk-mitigation measures described in Annex 3.

3.5 Instructions going beyond the Main Agreement must be given in text form and addressed to datos@decaportal.es. If they entail significant additional effort, G4F may request reasonable remuneration; the parties shall agree in advance on feasibility and effort.

3.6 If G4F is of the opinion that an instruction infringes data protection provisions, G4F shall inform the Controller without undue delay. G4F is entitled to suspend the execution of the instruction concerned until it has been confirmed or amended by the Controller.

4. Obligations of G4F

G4F undertakes:

4.1 to process personal data exclusively within the framework of this DPA and of the Controller's instructions;

4.2 to ensure that the persons authorised to process the data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and to train those persons in the handling of personal data;

4.3 to take and maintain the technical and organisational measures required under Article 32 GDPR; the measures taken are described in Annex 3. G4F may develop these measures further, provided that the agreed level of protection is not reduced;

4.4 to assist the Controller by appropriate technical and organisational measures in fulfilling its obligation to respond to requests from data subjects (clause 9);

4.5 to assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to G4F;

4.6 to inform the Controller without undue delay if a supervisory authority or another authority conducts investigations at G4F that may concern the Controller's data;

4.7 to document the processing activities carried out on behalf of the Controller in accordance with Article 30(2) GDPR.

5. Obligations of the Controller

5.1 The Controller is responsible for the lawfulness of the processing, for the existence of a legal basis and for safeguarding the rights of the data subjects.

5.2 The Controller shall inform the data subjects in accordance with Articles 13 and 14 GDPR. This applies in particular to drivers and to contact persons of shippers, consignees and other parties involved whose data are not collected from them directly.

5.3 The Controller shall enter into the Platform only such personal data as are necessary for the respective purpose. The entry of special categories of personal data within the meaning of Article 9 GDPR is not envisaged and must be refrained from.

5.4 The Controller administers the access authorisations of its users on its own responsibility and revokes them without undue delay as soon as the conditions for them cease to apply.

5.5 The Controller shall inform G4F without undue delay if, when reviewing the processing results, it identifies errors or irregularities.

6. Sub-Processors

6.1 The Controller grants G4F general written authorisation to engage further processors in accordance with Article 28(2) GDPR.

6.2 The sub-processors engaged at the time of conclusion of the contract are listed in Annex 2. The Controller authorises their engagement upon conclusion of this DPA.

6.3 G4F shall inform the Controller at least 30 days before the addition of a new sub-processor or the replacement of an existing one, in text form or by notice in

the customer account.

6.4 The Controller may object to the change within 30 days of receipt of the notification, in text form and on important data protection grounds. The objection must state reasons.

6.5 In the event of a justified objection, the parties shall seek a solution by mutual agreement. If no such solution is reached within 30 days and G4F cannot reasonably provide the service concerned without the sub-processor, either party is entitled to terminate the Main Agreement with effect as of the date on which the change takes effect. Fees already paid for the unused period shall be refunded on a pro-rata basis.

6.6 G4F shall contractually bind each sub-processor to data protection obligations that are substantially equivalent to the obligations under this DPA, and is liable to the Controller for their compliance in accordance with clause 13.

6.7 Ancillary services that G4F obtains from third parties and that are not directed at the processing of the Controller's personal data, such as telecommunications services, maintenance, cleaning or the disposal of data carriers, do not constitute sub-processing. G4F shall nevertheless take appropriate measures to safeguard the security of the data in these respects as well.

7. Places of Processing

7.1 The application and database infrastructure is operated in data centres within the European Union.

7.2 G4F shall notify the Controller of any relocation of the processing to another country in accordance with the procedure set out in clause 6.3.

8. Transfers to Third Countries

8.1 Personal data are processed outside the European Economic Area only insofar as the requirements of Articles 44 et seq. GDPR are met, in particular on the basis of an adequacy decision or the standard contractual clauses of the European Commission, supplemented by any necessary additional safeguards.

8.2 The sub-processors concerned and the safeguard applied in each case are identified in Annex 2.

8.3 G4F shall provide the Controller with information on the safeguards applied upon request.

9. Data Subject Rights

9.1 If a data subject contacts G4F directly in order to assert rights in relation to data that G4F processes on behalf of the Controller, G4F shall forward the request to the Controller without undue delay and shall not respond to it itself.

9.2 G4F shall assist the Controller in complying with requests for access, rectification, erasure, restriction, portability and objection, insofar as this is not possible, or possible only with disproportionate effort, without G4F's cooperation. For this purpose, the Platform provides the Controller with functions for searching, downloading, deleting and re-uploading.

9.3 G4F may request reasonable remuneration for assistance that goes beyond the functions provided by the Platform.

10. Personal Data Breaches

10.1 G4F shall inform the Controller without undue delay, and in any event within 48 hours of becoming aware, of any personal data breach affecting the Controller's data.

10.2 The notification shall contain, to the extent known, a description of the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a point of contact. Missing information shall be provided in phases.

10.3 G4F shall assist the Controller in complying with its notification and communication obligations under Articles 33 and 34 GDPR.

10.4 Notifications to the supervisory authority and communications to data subjects shall be made exclusively by the Controller, unless the parties agree otherwise in an individual case.

11. Evidence and Audits

11.1 G4F shall demonstrate compliance with the obligations under this DPA upon request, primarily by means of current attestations, certifications, reports of independent auditors or a completed self-assessment questionnaire.

11.2 If such evidence is insufficient in an individual case, the Controller may carry out an audit, or have one carried out by an auditor appointed by it who is bound to confidentiality and who must not be a competitor of G4F.

11.3 Audits shall be carried out upon at least 30 days' notice, during usual business hours, without disrupting operations, and no more than once per calendar year. Where there is justified suspicion of a material breach, or following a notifiable breach, the restrictions as to frequency and notice period do not apply.

11.4 The Controller shall bear the costs of any audit it initiates. Reasonable remuneration may be charged for G4F's effort, unless the audit reveals a breach on the part of G4F.

12. Deletion and Return upon Termination

12.1 Following termination of the Main Agreement, G4F shall make the data processed on the Controller's behalf available to the Controller for retrieval and download for a period of 15 months from the upload of the respective document. This period is based on the express instruction under clause 3.3(c) and serves to enable the Controller to comply with its statutory retention obligations.

12.2 The Controller may at any time instruct the early deletion of individual data or of the entire data set. G4F shall carry out the deletion within 30 days and confirm it in text form.

12.3 Upon expiry of the period under clause 12.1, G4F shall delete the data processed on the Controller's behalf. Notice of the deletion shall be given at least 30 days in advance and confirmed in text form upon request.

12.4 Backup copies are deleted in accordance with G4F's regular backup cycles, but no later than 90 days after deletion in the production system. Until then, they remain protected by the measures under this DPA and are not restored, except for the purpose of recovery following a system failure.

12.5 Storage beyond the above periods takes place only insofar as G4F is required to retain the data under Union or Member State law. In such a case, the processing remains limited to the retention purpose.

13. Liability

13.1 Liability as between the parties is governed by the provisions of the General Terms and Conditions.

13.2 Liability towards data subjects and the provisions of Article 82 GDPR remain unaffected.

13.3 If claims are asserted against a party on account of a breach of data protection provisions, the parties shall assist one another in defending such claims

and shall indemnify each other to the extent corresponding to their respective share of responsibility.

14. Confidentiality

The parties shall treat as confidential all information of the other party obtained in the course of this DPA. This obligation applies for the term of this DPA and for three years thereafter.

15. Amendments to this DPA

15.1 G4F may amend this DPA and its annexes insofar as this is necessary in order to adapt to changed legal requirements, to decisions of supervisory authorities or to technical developments. An amendment must not reduce the agreed level of protection.

15.2 Amendments shall be announced at least 30 days before they take effect, in text form or by notice in the customer account.

15.3 In the case of an amendment that affects the Controller's interests other than insignificantly, the Controller may terminate the Main Agreement free of charge, before the amendment takes effect, with effect as of that date; fees already paid for the unused period shall be refunded on a pro-rata basis.

15.4 By way of derogation, amendments to Annex 2 are governed by clause 6.

16. Final Provisions

16.1 In the event of contradictions between this DPA and the other contract documents, this DPA shall prevail in matters of data protection.

16.2 The invalidity of individual provisions does not affect the validity of the remaining provisions. The invalid provision shall be replaced by the legally permissible arrangement that comes closest to the purpose of the invalid provision.

16.3 The language of the contract, the applicable law and the place of jurisdiction are governed by the General Terms and Conditions. Mandatory data protection provisions remain unaffected.

Annex 1 – Subject Matter and Details of the Processing

Subject matter of the processing

Provision of a software-as-a-service solution for the creation, uploading, storage, provision, transmission and retention of electronic control documents for road haulage which are generated by the Controller in its own systems or in the Platform.

Nature of the processing

Collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure by transmission, making available, restriction, erasure and destruction.

Purpose of the processing

Compliance with the documentation obligations incumbent upon the Controller in road haulage, provision of the documents to Drivers and to enforcement authorities, and retention of the documents.

Categories of data subjects

- users of the Controller (employees, dispatchers, administrative staff);
- Drivers, including self-employed carriers;

- contact persons of shippers, consignees, principals and other parties involved in the carriage.

Categories of personal data

- **master data:** first name and surname, company affiliation;
- **contact data:** business email address, business telephone number;
- **employment-related data:** allocation to orders and carriages;
- **vehicle and carriage data with a personal reference:** registration numbers, driver allocation, loading and unloading locations, times;
- **document content:** all particulars contained in the control documents;
- **usage and log data:** log-in times, IP address, time stamps of upload and modification.

Special categories of personal data

Not envisaged.

Annex 2 – Sub-Processors

- **Supabase:** Database, authentication, storage of application data, Frankfurt, Germany
- **Alwyzon:** Hosting of the application, Austria
- **Helloly:** Hosting of the website decaportal.es, Austria
- **Infobip:** Delivery of email, SMS and messenger messages, European Union

Stripe acts as an independent controller for payment processing and is therefore not a sub-processor within the meaning of this DPA.

Annex 3 – Technical and Organisational Measures

Confidentiality

Physical access control: processing exclusively in certified data centres of the providers engaged, with access control, video surveillance and visitor management.

System access control: individual user accounts, password policies, multi-factor authentication for administrative access, automatic lock-out on inactivity.

Data access control: role-based authorisation concept based on the principle of least privilege, tenant separation, logging of administrative access.

Separation control: logical separation of data by customer, separate environments for development, testing and production, no use of production data for testing purposes.

Pseudonymisation and encryption: encryption of transmissions using TLS 1.2 or higher, encryption of stored data, formation of the Retrieval Addresses for control documents using random identifiers with high entropy that cannot be derived, exclusion from indexing by search engines, deactivation of public retrieval upon expiry of the designated period.

Integrity

Transfer control: encrypted transmission, documented interfaces, contractual commitment of sub-processors.

Input control: logging of the upload and modification of documents with a time stamp and the user account that triggered it.

Availability and resilience

- regular, encrypted data backups with verified restorability;

- redundant infrastructure of the providers engaged;
- monitoring of system status and load;
- documented procedure for recovery following outages.

Procedures for regular review

- documented procedure for handling personal data breaches, including reporting channels and deadlines;
- record of processing activities pursuant to Article 30(2) GDPR;
- data protection by default and data minimisation in the design of new functions;
- regular review of the effectiveness of the measures, updating of dependencies and security updates;
- commitment of all persons involved in the processing to confidentiality, and regular training.

Last updated: 1 October 2026