

Privacy Policy

Go4Future Consulting e.U. – DeCA Portal

Version: October, 1st 2026

1. Controller and Contact

The controller within the meaning of the General Data Protection Regulation (GDPR) is:

Go4Future Consulting e.U. Dr. Rudolf Klafsky-Straße 18, 2500 Baden, Austria Email: datos@decaportal.es Telephone: +43 660 240 48 09

Contact for data protection matters: Dr Thomas Leopoldseder, datos@decaportal.es

We have not appointed a data protection officer, as the conditions of Article 37 GDPR are not met.

2. Scope

This Privacy Policy applies to the website decaportal.es, to the application app.decaportal.es and to the related services. It provides information about the processing of personal data for which we are ourselves responsible, and about the distinction from those processing operations that we carry out on behalf of our customers.

3. Allocation of Roles

3.1 Our own controllership. We are the controller for the processing of data of our prospective customers, customers and their users, as well as for the operation of the website. These processing operations are described in clause 4.

3.2 Processing on behalf of a controller. For the content that our customers upload, transmit and store via the Platform, in particular the data of drivers, contact persons of shippers, consignees and other parties involved contained in the control documents, the respective customer is the controller. In that respect, we act as a processor (clause 5).

4. Processing Operations Carried Out under Our Own Responsibility

4.1 Provision of the Website and Server Logs

When you access our website, we process the IP address, the date and time of access, the page accessed, the volume of data transferred, the referrer as well as browser and operating system information.

Purpose: technical provision, system security, error analysis and prevention of abusive access. Legal basis: Article 6(1)(f) GDPR, legitimate interest in secure and stable operation.

4.2 Contacting Us

If you contact us via the contact form, by email or by telephone, we process your name, the name of your company, your email address, your telephone number where applicable, and the content of your enquiry.

Purpose: handling and responding to the enquiry. Legal basis: Article 6(1)(b) GDPR for pre-contractual enquiries, otherwise Article 6(1)(f) GDPR.

4.3 Pre-Registration and Waiting List

In the case of a pre-registration, we process contact details, company information and the date of registration. We will subsequently inform you about the options for using the Platform, in particular about the date of availability. Pre-registration may be linked to a benefits programme and does not give rise to any obligation to conclude a contract.

Purpose: preparation of the business relationship and information about availability.
Legal basis: Article 6(1)(b) GDPR as a pre-contractual measure.

4.4 Referral Programme

If we operate a referral programme, we process information about who has passed on a promotional code or referral link, who has registered through it and what benefits arise from it.

Purpose: administration and settlement of the benefits programme. Legal basis: Article 6(1)(b) GDPR.

There is no obligation to introduce or permanently maintain a referral programme.

4.5 Registration, Account Administration and Contract Performance

For the setting up and administration of customer accounts and user access, we process names, business email addresses, telephone numbers, company data including tax numbers, authorisations as well as usage and log data.

Purpose: contract performance, authentication, rights management, traceability of changes. Legal basis: Article 6(1)(b) GDPR; with regard to logging, Article 6(1)(f) GDPR.

4.6 Payment Processing

For the processing of payments, we process invoicing data, subscription data and payment status. The actual payment data are processed by our payment service provider; we do not receive any payment instrument data.

Purpose: billing of fees and compliance with tax obligations. Legal basis: Article 6(1)(b) and (c) GDPR.

4.7 System Communications and Support

For registration confirmations, system notifications, password resets, transaction messages, security notices and support enquiries, we process email addresses, telephone numbers, message content and technical metadata such as time and delivery status.

Purpose: technical provision of the communication functions and customer care. Legal basis: Article 6(1)(b) GDPR and Article 6(1)(f) GDPR.

4.8 Promotional Communications

We send information about products, new features and industry topics only to recipients who have given separate, express consent for this, or in the context of an existing customer relationship to the extent permitted by law.

Purpose: direct marketing. Legal basis: Article 6(1)(a) GDPR; for existing customers, Article 6(1)(f) GDPR.

Consent may be withdrawn at any time via the unsubscribe link in each message or by email to datos@decaportal.es. Withdrawal does not affect the lawfulness of the processing carried out up to that point.

4.9 Security and Prevention of Abuse

We process access and log data in order to detect, contain and investigate security incidents and abusive use.

Legal basis: Article 6(1)(f) GDPR.

4.10 Compliance with Legal Obligations

We process personal data insofar as this is necessary in order to comply with obligations under tax, accounting and company law.

Legal basis: Article 6(1)(c) GDPR.

5. Processing on Behalf of Our Customers

5.1 Where a customer uses the Platform to create, upload, transmit and retain control documents, those documents may contain personal data of third parties, in particular of drivers, contact persons of shippers and consignees, and other parties involved in the carriage.

5.2 The customer is the controller for such data. We process them exclusively on the customer's documented instructions on the basis of a data processing agreement pursuant to Article 28 GDPR. That agreement governs in particular the subject matter and duration of the processing, the categories of data subjects and of data, the technical and organisational measures, the engagement of further processors, the support provided to the customer in relation to data subject requests, and the deletion or return of the data after the end of the contract.

5.3 Data subjects whose data are processed in this context should contact the respective customer as controller in order to exercise their rights. We will forward requests received directly by us to the customer without undue delay.

5.4 The customer is responsible for informing the data subjects in accordance with Articles 13 and 14 GDPR, in particular drivers whose data are not collected from them directly.

6. Retrieval of Control Documents via a Unique Web Address

6.1 The applicable provisions require that every electronic control document has a unique web address which, during roadside checks, allows it to be downloaded directly without any additional log-in. This means that the file, which may contain information about drivers, vehicle registration numbers and the undertakings involved, is accessible to any person who has that address or the associated QR code.

6.2 The control documents are generated by our customers, either in their own systems and then uploaded to the Platform, or in the Platform itself from the particulars they enter, where applicable completed by a driver they have invited. Before an uploaded document we place a cover page containing the QR code with the retrieval address as well as the date and time of the upload; the content of the pages transmitted by the customer is not altered. A control document generated in the Platform carries the QR code and the time details on the document itself.

6.3 In order to limit the associated risks, we apply the following measures: formation of the addresses using random identifiers with high entropy that are neither derivable nor enumerable; transmission exclusively via HTTPS using TLS 1.2 or higher; exclusion from indexing by search engines; and deactivation of public retrieval upon expiry of the designated period, while the document remains available to the customer in its protected area.

6.4 The legal basis is compliance with a legal obligation of the customer (Article 6(1)(c) GDPR) as well as performance of the contract between the customer and us (Article 6(1)(b) GDPR).

7. Recipients and Processors

We disclose personal data only to the following categories of recipients:

7.1 Communication services. For the delivery of SMS, WhatsApp and email messages as well as authentication and system messages, we use Infobip. Processing takes place in data centres within the European Union. The data

processed are telephone numbers, email addresses, message content and technical metadata.

7.2 Database and backend infrastructure. Our Platform runs on a cloud infrastructure with database and authentication services provided by Supabase. The data processed are user data, application data and document information. Processing takes place in data centres within the European Union, specifically in Frankfurt (Germany).

7.3 Website and application hosting. The content of the domain decaportal.es is hosted with Helloly, and the application with Alwyzon. Processing takes place in data centres in Austria.

7.4 Payment service provider. For payment processing, we use Stripe. Stripe processes payment data as an independent controller. We have no access to your payment instrument data.

7.5 Analytics and advertising. Only where consent has been given do we use Google Analytics, Google Ads conversion tracking and the LinkedIn Insight Tag for LinkedIn conversion tracking (clause 9).

7.6 Advisers and authorities. We disclose data to tax advisers, legal representatives and auditors as well as to authorities and courts insofar as this is required by law or necessary for the establishment, exercise or defence of legal claims.

Agreements pursuant to Article 28 GDPR are in place with all processors. We do not sell personal data and do not disclose them for the advertising purposes of third parties.

8. Transfers to Third Countries

Individual service providers may process data outside the European Economic Area, in particular in the area of analytics and advertising services and payment

processing. In such cases, we base the transfer on the standard contractual clauses adopted by the European Commission and, where applicable, on an adequacy decision, supplemented by additional safeguards.

9. Cookies and Audience Measurement

9.1 We use technically necessary cookies which are required for the operation of the website and the Platform. These do not require consent.

9.2 In addition, subject to prior consent given via our cookie banner, we use analytics and advertising cookies, in particular Google Analytics, Google Ads conversion tracking and the LinkedIn Insight Tag, in order to evaluate the use of the website and to measure the effectiveness of our campaigns.

9.3 These cookies are set only after you have given your consent. You may withdraw your consent at any time, just as easily as you gave it, via the “Cookie settings” link in the footer of the website.

9.4 Details of the individual cookies, their purpose, their provider and their storage period can be found in our [Cookie Policy](#).

10. Storage Periods

- Customer account and contact data: For the duration of the account, thereafter 12 months
- Control documents and their metadata: 12 months from upload, subject to any diverging instruction from the customer acting as controller
- Invoicing and accounting records: In accordance with the statutory retention periods
- Pre-registrations without a subsequent contract: 12 months from registration

- Support communications: 12 months from closure
- Server logs and IP addresses: 6 months, unless required to investigate a security incident
- Data based on consent: Until withdrawal

Upon expiry of the periods stated, the data are deleted or anonymised.

11. Security

We take appropriate technical and organisational measures pursuant to Article 32 GDPR, in particular encryption of transmissions by means of TLS, encryption of stored data, role-based access control, authentication of users, logging of access, regular data backups and a regular review of the effectiveness of these measures.

12. Your Rights

You have the right to:

- access to the data processed about you;
- rectification of inaccurate data;
- erasure;
- restriction of processing;
- data portability;
- object to processing based on a legitimate interest;
- withdraw consent given, without affecting the lawfulness of the processing carried out up to that point.

To exercise these rights, please contact datos@decaportal.es. We may request additional information in order to verify your identity.

You also have the right to lodge a complaint with a supervisory authority. Our lead supervisory authority is the Austrian Data Protection Authority (Österreichische Datenschutzbehörde), Barichgasse 40–42, 1030 Vienna, dsb@dsb.gv.at. Persons resident in Spain may also contact the Spanish Data Protection Agency, Agencia Española de Protección de Datos (www.aepd.es).

13. Necessity of Providing Data

The provision of the data required for the conclusion of the contract and for account administration is necessary in order to be able to use the Platform. Without these data, no contract can be concluded and no access can be provided. The giving of consent is voluntary and is not required in order to use the Platform.

14. No Automated Decision-Making

No automated decision-making, including profiling, that produces legal effects concerning you or similarly significantly affects you takes place.

15. Amendments to this Privacy Policy

We update this Privacy Policy when the processing operations, the service providers engaged or the legal situation change. The version published on this website applies from time to time.

Last updated: October, 1st 2026