

FAQ about GDPR in Consignor

Version 1.1

20.05.2018

This document seeks to answer frequently asked questions about Consignor's Data Processing Agreement ([Consignor Terms of Use](#)) and GDPR in Consignor.

1.0 Consignor terminology

1.1 What does the term "Consignor Platform" cover?

The term "Consignor Platform" refers to all existing and future parts of the Consignor Software, including all versions of the software and all add-on services provided to the basis software.

Examples (non-exhaustive list):

- Consignor On-Premises
- Consignor Ticket
- Consignor Shipment Server
- Consignor Portal
- Scan App
- Online Return Services
- Etc.

1.2 What is Consignor Terms of Use?

Consignor Terms of Use constitutes the agreement between the customer legal entity ("Customer") and the Consignor local legal entity. The Terms of Use governs the Customer's access to and use of the Consignor Platform, and Consignor's delivery of ancillary goods or services.

Consignor Terms of Use also governs the processing of personal data carried out by Consignor in connection with the delivery, and therefore constitutes the contract (Data Processing Agreement) between Consignor and the Customer as required under the GDPR Article 28 No. 3.

1.3 What is Consignor Data Processing Agreement?

Consignor Terms of Use governs the processing of personal data. Consignor Data Processing Agreement (Consignor Terms of Use) do not have to be signed by the customer.

1.4 What is Consignor Privacy Policy?

Consignor Privacy Policy explains what kind of information we collect when you communicate with us or visit one of our websites, how we collect it and why. It also explains the specific ways we use and disclose that information.

2.0 GDPR terminology

2.1 What is GDPR?

GDPR is an abbreviation of General Data Protection Regulation, which is a regulation that is issued by EU/EEA and enters into force 25th May 2018.

Consignor publish all relevant documentation regarding GDPR online:
www.consignor.com/data-security

2.2 What is personal data?

Personal data is any information that relates to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the law.

Personal data that has been rendered anonymous in such a way that the individual is no longer identifiable is not considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

The law protects personal data regardless of the technology used for processing that data – it is technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria. It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper; in all cases, personal data is subject to the protection requirements set out in the GDPR.

Examples of personal data:

- Name
- Home address
- Personal e-mail address (e.g. name@company.com)
- Phone no.
- Internet Protocol (IP) address
- Cookie ID

Examples of data NOT considered personal:

- Company registration no.
- General e-mail address (e.g. info@company.com)
- Anonymised data

A complete list of the types of personal data Consignor processes is available for download at www.consignor.com/data-security

2.3 What is sensitive personal data?

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is considered sensitive and generally not allowed to process, except where certain conditions are met.

Shipment Data transferred to Consignor does not include sensitive personal data.

2.4 What is Data Subject?

A Data Subject is a living individual to whom personal data relates.

2.5 What is a Data Controller?

A Data controller is the one that determines the purposes and means of the processing of personal data.

Consignor's customers are data controllers of personal data collected and processed within the Consignor Platform (shipment data).

Consignor is the data controller of personal data collected about Consignor's customers, partners and employees.

2.6 What is a Data Processor?

Data processor is the one who processes personal data on behalf of the Data Controller.

Consignor is the data processor of our customer's data processed within the Consignor Platform (shipment data).

2.7 What is Consignor's purpose of processing personal data?

Personal data will only be collected and processed if there are a specified, explicit and legitimate purposes for it. Moreover, personal data will not be further processed in a manner that is incompatible with those purposes.

When Consignor processes personal data the purpose is to fulfil the contract which the customer has signed with Consignor. The terms for data processing in this regard is stated in [Consignor Terms of Use section 7.1 and 7.2](#).

Where Consignor collect and processes data upon consent (e.g. newsletter signup) the purpose will be addressed in the specific situation. As well as clear information about withdrawal of the consent will be presented before the consent is given. The policy for data processing in this regard is stated in Consignor's [Privacy Policy](#).

2.8 What are the rights of the Data Subject?

Since the Data Subject is the owner of the data he/she has several rights which can be invoked to the Data Controller:

- **Right to access**
If asked, Consignor will inform the data subject whether it has personal data about the data subject, and will give the data subject access to the personal data.
- **Right to rectification**
When notified by the data subject, Consignor will correct all incorrect personal data and will complete any incomplete personal data.
- **Right to data portability**
The data subject has the right to receive the personal data concerning him or her in a structured, commonly used and machine-readable format, and has the right to transmit this data to another organisation.
- **Right to object**
If a data subject objects to the processing of his or her personal data, Consignor will cease processing the data, unless Consignor can demonstrate that there are legitimate reasons to process the data.
- **Right to be forgotten**
When there are no longer any legitimate reasons for Consignor to keep personal data about a data subject, the data will be erased. This includes the situation where the data subject withdraws consent to keep the data.

These rights can only be invoked to the Data Controller so in cases where Consignor is Data Processor (e.g. Shipment Data) the Data Subject must address the Data Controller (Consignor's customer) who can manage all personal data directly in Consignor Portal.

In cases where Consignor is the Data Controller the Data Subject can send a request to Consignor's DPO to invoke the rights. Moreover, Consignor have controls in place to remove personal data when the purpose for processing is no longer present.

Please see section 2.4 for a clarification of the Data Controller and Data Processor terms.

2.9 How long does Consignor process the personal data?

Consignor will not process personal data any longer than necessary. The retention periods can differ based on the type of data processed, the purpose of processing or other factors.

A complete list of the types of personal data Consignor processes and the retention period is available for download at www.consignor.com/data-security

2.10 Do Consignor have an Information Security Management System?

Yes, Consignor has implemented appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. These measures are reviewed and updated at regular intervals.

Moreover, Consignor is in the process of being ISO27001 certified.

2.11 Are there any requirements for the collaborators which Consignor transfer data to?

Yes, if Consignor lets others process personal data, only providers who can do so in accordance with the GDPR will be used.

Consignor ensures that a risk assessment, Data Processing Agreements and any necessary acceptance from customers are in place before letting others process personal data.

Moreover, Consignor will have a contract with any providers that process personal data for it. The contract will describe the following:

- The subject matter of the processing
- The duration of the processing
- The nature and purpose of the processing
- The type of personal data and categories of data subjects
- Consignors obligations and rights

Consignor have Data Processing Agreements in place with all providers that process personal data.

2.12 Do Consignor cooperate with the any supervisory authority?

Yes, when necessary Consignor and its providers will cooperate with the personal data supervisory authorities. Since Consignor's head quarter is placed in Oslo the Norwegian supervisory authority, Datatilsynet (www.datatilsynet.no), is the natural point of contact.

2.13 What happens if a personal data breach occurs?

Consignor has procedures for data breach handling. In the case of a personal data breach, Consignor will, as soon as possible and within 72 hours after having become aware of it, notify the breach to the supervisory authority, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it will be accompanied by reasons for the delay.

The notification will:

- describe the nature of the personal data breach
- communicate the name and contact details of the data protection officer
- describe the likely consequences of the personal data breach
- describe the measures taken or proposed to be taken by Consignor

Consignor have implemented a Business Contingency Plan which is part of the ISO27001 certification. Consignor does also have routines in place to handle information towards supervisory authority.

2.14 Do you notify the data subject if you have a personal data breach?

Yes, if the personal data breach is likely to result in a high risk to natural persons, Consignor will communicate the personal data breach to the data subjects without undue delay.

Consignor have routines in place to handle information towards data subjects.

2.15 Do Consignor have a designated DPO?

Yes, Consignor has appointed a designated DPO (Data Protection Officer). All relevant contact information will be published on Consignors [website](#) and communicated to the supervisory authority.

2.16 What if Consignor transfer data outside the EU/EEA?

If and when Consignor transfers data outside of the EU/EEA, all provisions given in the GDPR will still be adhered to.

2.17 Are transfers subject to appropriate safeguards?

Yes, in the case where the commission has not made any adequacy-based decision that a third-party country is safe, Consignor will only transfer personal data outside of the EU/EEA if Consignor has provided appropriate safeguards, and if enforceable personal data rights and effective legal remedies are available.

2.18 How do I receive more information about Data Security?

If you would like to receive information about changes, updates etc. in relation to data security in Consignor, please sign up for our [Data Security Information Letter](#) via.

2.19 What if a data subject of the controller contacts Consignor directly?

In the event that a data subject of the Controller (e.g. a person that has received a package generated by a Consignor Customer on the Consignor platform) contacts Consignor (as a Data Processor) and ask for information about the status of their personal data, Consignor will refer the Data Subject to the Controller. By that it is always the Controller that controls the data and/or delete personal data on behalf of their Data Subjects.

2.20 What about audits and inspections?

Consignor offers different types of audit packages, that are tailor-made to both demonstrate compliance with the obligations lead down and to ensure that individual Customer's audit needs are met:

	Basic	Extended	Enterprise
Price/year	Euro 0	Euro 1,000	Euro 5,000
Yearly Audit Report	On request	On request	On request
Data Security Information Letter	Yes. Sign up.	Yes. Sign up.	Yes. Sign up.
Data Security Webinar by DPO	Not available	Yes.	Yes.
1 x 2 hour phone audit between DPO and Customer representatives	Not available	Yes.	Yes.
1 x 1-day onsite audit at Consignor sites including attendance from DPO and Key Account Manager	Not available	Not available	Yes.
Sub-supplier audit report	On request	On request	On request