GDPR Supplier

Privacy Notice

DANX Carousel

Table of Contents

GDPR Group Supplier Privacy

1. Introduction

The DANX Carousel Group of companies (hereafter "The Group," "We," "Our") is a time critical service logistics and supply chain specialist with strong positions in the UK, EU - Ireland, Benelux, DACH, Iberia, Nordics, Baltics, Poland and EEA - Norway.

The Group consists of DANX, DANX ILS, UT, TBS, FOMAB, TLS Group, LPR Group, Carousel, Alltrans, Logik and LPR.

The Group is a comprehensive partner for logistics and supply chain services such as time-critical spare parts distribution, warehousing, final mile, linehaul, battery logistics, customs clearance, and more.

GDPR correspondence address DANX A/S: Vejleåvej 9 2635 Ishøj

2. Purpose and scope

This privacy notice outlines how we collect, use, and protect personal data for suppliers. This notice complies with the UK GDPR, EU GDPR, EEA countries and their national applicable data protection laws.

3. Roles and responsibilities

We are committed to ensuring GDPR compliance across our organisation. Where we are the Data Controller, we determine the purposes and means of processing personal data. e.g. why and how personal data is processed and have sole control over how the data is processed. Where the supplier is the Data Controller, they determine the purposes and means of processing personal data. e.g. why and how personal data is processed and have sole control over how the data is processed.

Where we are the Data Processor, we process personal data on behalf of the controller at the controller's instructions and will not engage with a sub processor without written consent, and the Data Controller reserves the right to perform an audit. Where the supplier is the data processor, they process personal data on behalf of the controller at the controller's instructions and will not engage with a sub processor without written consent, and the Data Controller reserves the right to perform an audit.

The Data Controller is fully liable for compliance, even when outsourcing to Data Processors and non-compliance can lead to joint liability with significant fines and reputational damage. Data Processor Agreements are in place for all suppliers that process data on our behalf.

We expect all suppliers who process data on our behalf to complete a due diligence questionnaire, sign a data processing agreement and acknowledge and adhere to the expectations outlined in our Supplier Code of Conduct.

4. Technical and security measures

We maintain an information security and privacy management framework proportionate to risk, designed to ensure the confidentiality, integrity, availability, and resilience of personal data processing. Organisational measures include governance and accountability structures (roles, policies, training), risk and DPIA processes, access control and least privilege, vendor and transfer controls, incident response and breach notification procedures, data lifecycle and retention management, regular testing and assurance (audits, vulnerability management, exercises), and business continuity/disaster recovery. Measures are reviewed, tested, and improved on an ongoing basis in line with GDPR Article 32 and the principle of privacy by design and default.

we support information security through our international standards 27001: 2022 and NIS2, this ensures our technical, organisational and security measures (e.g. encryption, access controls) are compliant.

5. Lawful bases for processing data

We will handle supplier data lawfully, fairly, and transparently and only process the necessary personal data provided directly by the supplier, such as name, address, contact details, bank details. solely for the purposes of managing suppliers.

Below are typical areas of the lawful bases for processing supplier data

Processing area	Examples of the lawful bases for processing
Performance of a Contract Article 6 (1)(b)	To manage supplier relationships (e.g. place and order, pay an invoice)
Legal Obligation Article 6 (1)(c)	To comply with the legal requirement. (e.g. tax compliance)
Legitimate Interest Article 6 (1)(f)	Managing business operations

6. Data transfers

We may on occasion transfer personal data to countries outside the UK/EU/EEA when this is necessary for the purposes described in this notice. Whenever we do so, we ensure that the information remains protected to the same standards required under the UK GDPR and EU GDPR.

We only transfer data where one of the following applies:

- the country has been recognised as providing an adequate level of data protection;
- we have put in place appropriate safeguards, such as Standard Contractual Clauses or the UK International Data Transfer Agreement; or
- an approved exception (derogation) applies in specific situations, such as when you have given explicit consent or the transfer is necessary for a contract.

Before making any international transfer, we assess the legal and security risks and apply measures such as encryption and strict access controls to keep your data safe.

We have third party data processing agreements in place and require the completion of a supplier due diligence questionnaire for all third-party Data Processors. We also include a summary of our expectations within our Supplier Code of Conduct to ensure compliance and to protect employee data.

7. Data retention

Data retention rules exist for several important reasons under GDPR and good governance practices**:**

1. **Legal Compliance -** Certain laws require organisations to keep data for a specific period (e.g., tax).
2. **Accountability & Audit -** Retention policies help demonstrate compliance with GDPR principles, especially **storage limitation** and **accountability**.
3. **Business Needs -** Some data must be retained for operational purposes (e.g., service history).
4. **Risk Management -** Keeping data longer than necessary increases risks of **data breaches**, **unauthorised access**, and **non-compliance fines**.
5. **Storage Limitation Principle (Article 5(1)(e)) -** GDPR requires that personal data be kept **no longer than necessary** for the purposes for which it was collected.

Depending on the data type and the category of data in the country in which it is held there are a variety of retention periods depending on the applicable GDPR clauses. A summary can be found in Appendix A

8. Deletion and destruction of data

Personal data is destroyed (or securely deleted) when it is no longer needed for the purpose it was collected.

Digital Data will be deleted and securely destroyed from all active systems, and this is carried out in accordance with the applicable data retention laws and data subject access requests and regulations in countries in which it operates. Hardware will be destroyed by appropriate methods where needed.

Paper Documents data destruction is carried out by appropriate methods e.g. via shredding bins and where appropriate for the destruction of bulk files by an authorised and regulated company for secure destruction. Paper records must be retained according to the company's Record Retention Schedule.

We conduct periodic audits to ensure compliance and identify gaps. Data that is subject to litigation or regulatory investigations must not be deleted or destroyed until formally released.

The deletion and destruction of data are also documented in our ISMS Document Control and Records Management Procedure.

9. Data Subject Rights (DSR)

Individuals have the right to access, rectify, erase ("right to be forgotten"), restrict, or object to the processing of their personal data, by contacting the Group Data Controller Officer, they also have the right to data portability and to withdraw consent and to be able to lodge a complaint if resolution can't be found, directly with the relevant supervisory authority (see Appendix B) or seek judicial remedy.

For further details please refer to our Data Subject Request Policy and Procedure or request a copy by emailing gdpr@danxcarousel.com

10. Reporting a data breach

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed — Article 4(12).

We will notify the appropriate supervisory authority based on the region the breach has happened within 72 hours of becoming aware of the breach where feasible or provide reasons for any delay. We will also notify any affected suppliers if the breach is likely to result in a high risk to their rights and freedoms, including giving advice on how they can protect themselves. We document all breaches within our internal GDPR system.

You can report a data breach to the Information Security Team via email on GDPR@danxcarousel.com

In the unlikely event that you are dissatisfied with the response, you can lodge a complaint directly with the relevant supervisory authority or seek judicial remedy.

Appendix A: Data retention schedule (EU & UK GDPR)

Data Category	Examples	Retention Period	Rationale / GDPR Basis
Customer Account & Contact Information	Name, email, phone, address	Duration of customer relationship + 6 years	GDPR requires defined, justified periods for customer/client data.
Communications & Support Queries	Emails, chat logs, support tickets	2 years from last contact	Communications logs require documented retention and deletion processes.
Financial & Transactional Records	Invoices, payments, purchase history	6 years	Retention aligned with legal and accounting obligations.
Marketing Data	Preferences, consent logs	Until consent withdrawn + 2 years	Need proof of consent and storage limitation compliance.
Website Analytics & Server Logs	IP addresses, cookies, device identifiers	12–24 months	Analytics data must have justified retention periods.
CCTV & Access Logs	Video recordings, entry logs	30–90 days	CCTV footage requires defined retention schedules.
Employee & HR Data	Contracts, HR files	6 years after employment ends	HR records require structured retention schedules.
Processor / Third-Party Data Handling	Any data processed externally	Only retained for period specified by controller	Processors must follow controller-defined retention schedules.

Appendix B: Supervisory authorities contact details

Country	Authority	Website
Denmark	Danish Data Protection Agency (Datatilsynet)	https://www.datatilsynet.dk/english
Sweden	Swedish Authority for Privacy Protection (IMY)	https://www.imy.se/en/
Norway	Norwegian Data Protection Authority (Datatilsynet)	https://www.datatilsynet.no/en/
Finland	Office of the Data Protection Ombudsman	https://tietosuoja.fi/en/home/
Estonia	Estonian Data Protection Inspectorate	https://www.aki.ee/en
United Kingdom	Information Commissioner's Office (ICO)	https://ico.org.uk/global/contact-us/
Ireland	Data Protection Commission (DPC)	https://www.dataprotection.ie/en/contact/how-contact-us
Germany	Federal Commissioner for Data Protection (BfDI)	https://www.bfdi.bund.de
Spain	Agencia Española de Protección de Datos (AEPD)	https://www.aepd.es
Iberia (Corporate)	Iberia Líneas Aéreas de España, S.A.	https://www.aepd.es

DANX Carousel

Review and revision of privacy notice

This privacy notice will be reviewed and revised annually for compliance to the privacy notice content or as required if changes to legislation apply sooner.

Contact

If you have any questions relating to the content of this privacy notice, please direct them to: gdpr@danxcarousel.com