Data Retention & Deletion Policy

Policy Statement

DANX Carousel

Data Retention & Deletion Policy

Contents

Data Retention & Deletion Policy

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.

2. Purpose and scope

This policy ensures that company data including personal data is retained only for as long as necessary to fulfil its intended purpose, retained only for legitimate business or legal purposes, deleted or anonymised when no longer needed and appropriate technical and organisational measures are applied during retention, in compliance with the DANX Carousel ISMS, EU GDPR (Art. 5(1)(e)), UK GDPR & Data Protection Act 2018 and EEA GDPR obligations
This policy applies to:

- All data (personal and non-personal) processed by the DANX Carousel Group
- All systems, applications, and storage media
- Employees, contractors, and third-party processors

3. Principles

Data retention rules exist for several important reasons under data privacy legislation, ISO and NIS2 information security compliance frameworks and good governance practices**:**

1. **Legal Compliance -** Certain laws require organisations to keep data for a specific period (e.g., tax records, employment records for statutory obligations).
2. **Accountability & Audit -** Retention policies help demonstrate compliance with information security and data protection principles, especially storage limitation and accountability**.**
3. **Business Needs -** Some data must be retained for operational purposes (e.g., warranty claims, 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.
6. **ISO27001:** 2022 – requires that Information stored in information systems, devices or in any other storage media shall be deleted when no longer required"

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 legislative clauses.

4. Deletion and destruction of data

Company information and data including personal data must be destroyed (or securely deleted/anonymised) when it is no longer needed for the purpose it was collected. This requirement comes from the storage limitation principle in the GDPR Article 5(1)(e).

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. Digital data must be retained in line with the retention periods set out for different types of data and varies by region, detail of which can be found online.

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.

5. Roles and responsibilities

We are committed to ensuring information security best practice and data privacy compliance across our organisation and have appointed key roles to monitor compliance and mitigate risk in this area.

The Data Protection Officer (CPO) is an external business advisor with expert knowledge of data protection laws and practices to ensure GDPR compliance.

The Data Controller Officer (DCO) oversees Group GDPR compliance, maintaining key documents and registers and conducts audits/risk assessments.

The Information Security team is responsible for the security measures needed to be compliant and overall management of data breaches.

The business units are responsible for applying the retention schedules in line with the correct data type and region

6. Governance and Review

This policy will be reviewed annually or as required by changes in legislation.

7. Adoption of Policy

The DANX Carousel Group's Data Retention and Deletion Policy statement was adopted and approved by the GDPR Executive Team Sponsor and Information Security team on 4th March 2026.

DANX Carousel

Review and revision of this policy

This policy will be reviewed and revised annually for compliance to the policy 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