GDPR Appropriate Policy Document

DANX Carousel

Table of Contents

GDPR Appropriate Policy Document

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 Appropriate Policy Document (APD) describes how the DANX Carousel Group protects special category data and criminal offence data under:

UK regulatory framework

- UK GDPR
- Data Protection Act 2018, including Schedule 1 conditions (where applicable)

EU / EEA regulatory framework

- EU GDPR (Regulation (EU) 2016/679) – Articles 9 and 10
- National implementation of laws in relevant EU Member States (where required)

The purpose of this APD is to demonstrate that our processing is:

- Lawful
- Fair
- Transparent
- Secure
- Necessary and proportionate

It sets out safeguards, retention rules, and accountability measures.

3. Lawful bases for processing data

We will handle personal data lawfully, fairly, and transparently and only process the necessary personal data provided directly by the data subject.

Under UK GDPR, processing requires an article 6 lawful basis and a schedule 1 DPA 2018 condition when processing special category data (article 9) and/or criminal offence data (article 10). Example of Schedule 1 Conditions used by us are employment, social security & social protection (Sch 1, para 1).

Under EU GDPR, processing requires an article 6 lawful basis and article 9 (2) condition for special category data such as explicit consent. Article 10 applies to criminal offence data requiring legal authorisation under member state law or complementary safeguards.

4. Categories of special category data

We may process the following, limited to what is necessary and proportionate:

Special category data (EU & UK)

- Health data
- Racial or ethnic origin
- Biometric data for identification
- Sexual orientation
- Religious or philosophical beliefs
- Trade union membership
- Genetic data

Criminal Offence Data

- Allegations
- Investigations
- Convictions
- Security/vetting information

5. Purposes of processing special category data

We process special category and/or criminal offence data under both UK and EU GDPR for purposes such as:

- Employment & workforce management
- Payroll, tax, and social security compliance
- Health & safety
- Wellbeing and occupational health
- Equality & diversity monitoring
- Safeguarding individuals
- Crime prevention and detection
- Legal claims and dispute resolution
- Research, analytics or statistical purposes (where appropriate and lawful)

6. Data retention

Data retention rules exist for several important reasons under GDPR and good governance practices**.** Retention is based on:

- Statutory obligations (UK & EU, EEA)
- National employment and health & safety laws
- Limitation periods for legal claims
- Data minimisation and necessity

At the end of the retention period, data is:

- Securely deleted,
- Anonymised, or
- Archived (where legally justified).

A data deletion and retention policy and retention schedule are maintained separately.

7. Safeguard and security measures

Our organisational safeguards include:

- Strict access controls (need-to-know)
- Confidentiality agreements for staff
- Regular data protection and security training
- Policy framework for security, retention, access and classification
- DPIAs for high-risk processing

Our technical safeguards include:

- Encryption
- MFA and privileged access controls
- Monitoring, logging, and audit trails
- Regular patching and vulnerability management
- Secure backup & disaster recovery processes

These align with: UK GDPR Article 5 & 32 and EU GDPR Article 5 & 32

8. Data sharing and transfers

We may on occasion transfer personal data to countries outside the UK/EEA, when we do so, we ensure that the information remains protected to the same standards required under the UK GDPR and EU GDPR. Transfers occur only where appropriate safeguards are in place.

Data may be shared with Processors under binding contracts**,** Occupational health providers**,** Insurers and advisors**,** Regulators and authorities (where required by law). International transfers follow UK GDPR Chapter V (UK Transfer Risk Assessment, IDTA, UK Addendum to SCCs) and EU GDPR Chapter V (EU Standard Contractual Clauses + Transfer Impact Assessment).

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 customer data.

9. Data subject rights

Individuals have the following rights under UK, EU and EEA GDPR:

- Access
- Rectification
- Erasure
- Restriction
- Objection
- Portability
- Rights related to automated decision-making
- Withdrawal of consent (where applicable)

Requests are handled under our Data Subject Request Procedure.

10. Accountability

We maintain documentation including:

- Records of Processing Activities (RoPA)
- Contracts with processors
- DPIAs
- Evidence of Schedule 1/DPA 2018 conditions (UK only)
- Data protection and security audits
- Staff training records
- Policies and procedures

Record-keeping ensures compliance with UK GDPR Article 5(2) and EU GDPR Article 5(2) (Accountability principle).

11. Review of document

This APD is reviewed as a minimum annually, if processing changes significantly or after changes to UK, EU or EEA data protection legislation.

12. Key contacts

Role	Contact Name	Contact details
Group Chief Privacy Officer (CPO)	Resolva Law	gdpr@danxcarousel.com
Group Data Controller Officer (DCO)	Alison Brindley	gdpr@danxcarousel.com
Information Security Team	N/A	gdpr@danxcarousel.com

DANX Carousel

Contact

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