GDPR Job Applicant

Privacy Notice

DANX Carousel

GDPR Job Applicant Privacy Notice

Contents

GDPR Job Applicant Privacy Notice

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 job applicants. This notice complies with the UK GDPR, EU GDPR, EEA countries and their national applicable data protection laws.

3. Technical and security measures

We maintain an information security and privacy management framework proportionate to risk, designed to ensure 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.

4. Lawful bases for processing data

As recruiters we will handle applicant data lawfully, fairly, and transparently and only process the necessary personal data provided directly by job applicants, agencies or background check providers, including: name, address, contact details, employment history, personal evaluations, work record, criminal convictions or offences, political, religious or philosophical beliefs and sexual orientation, solely for the purposes of recruitment. Below are typical areas of the lawful bases for processing job applicant data.

Processing area	Examples of the lawful bases for processing
Consent Article 6 (1)(a)	The applicant has given clear informed and specific permission for their data to be processed, permission is given freely, and the data subject can withdraw consent at any time. (e.g. for optional data like diversity monitoring)
Legal Obligation Article 6 (1)(c)	Processing is necessary to comply with the legal requirement. (e.g. right to work checks)

GDPR Article 9 regulates the processing of special category personal data, which includes: racial/ethnic origin, political opinions, religion, trade union membership, genetics, biometrics, health, sex life, and sexual orientation. Because this data is highly sensitive, the GDPR requires two things:

1. A standard lawful basis under Article 6, *and*
2. A specific condition for processing under Article 9(2).

Our standard lawful basis for processing job applicant data within HR is: Legal Obligation — Article 6(1)(c)
Our specific condition for processing is: Employment, Social Security & Social Protection — Article 9(2)(b)

We do not use or apply automated decision-making and profiling for recruitment or job application screening; however, we may use automated decision-making and profiling through a third-party provider for purposes such as fraud and criminal activity detection with respective authorities and regulators at the recruitment stage, you will be advised prior if this is required. Individuals have the right to request human intervention, express their point of view, and contest decisions.

5. Consent for processing personal data

We process certain personal data based on your consent, as required under GDPR (Article 7 UK/EU GDPR). This means you have a genuine choice and control over whether we use your information for these purposes. Consent is freely given, specific, informed, and unambiguous, and individuals can withdraw consent as easily as it was given.

What are you consenting to?
When you provide consent, you agree that we may process your personal data for the specific purposes described at the point of collection, such as:

- Optional data like diversity monitoring
- Sharing data with named third parties for agreed purposes (e.g. Criminal record checks)

Your rights

- **Voluntary**: Giving consent is entirely optional
- **Withdrawal**: You can withdraw your consent at any time without affecting the lawfulness of processing before withdrawal. To withdraw**,** please email us at gdpr@danxcarousel.com, update your preferences in your account settings, or click the unsubscribe link in our communications

Granular choices
Where we ask for consent for multiple purposes, you will be able to choose which purposes you agree to and which you do not.

Record keeping
We maintain records of:

- Who consented
- When and how consent was given
- The wording presented at the time
- Any withdrawal of consent

6. Data transfers

Data may be shared with external parties for the purposes of the recruitment process. (e.g. background check providers, regulators). This will be done in line with the GDPR guidelines.

We may on occasion transfer personal data to countries outside the UK/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 job applicant data.

You can contact us if you would like more information about international transfers or to request a copy of the applicable safeguards via gdpr@danxcarousel.com

7. Data retention

Job applicant data is only used for the purposes of the recruitment process and retained in accordance with the relevant guidelines for the appropriate region (e.g. in the UK, an unsuccessful applicants' data is retained no longer than 6 months unless consent is given to retain longer, whereas successful applicants' data may be retained for up to 6 years).

You can find a general retention period schedule 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.

The destruction of **Paper Documents** 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.

Because special category data is higher risk, the GDPR requires stricter controls. Special category data is retained only for the minimum period necessary for its purpose, justified by legal or operational requirements, and documented in our retention schedule and Appropriate Policy Document. Data is securely erased or anonymised once no longer required, and regular review cycles ensure compliance with storage limitation and accountability obligations.

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

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.

Please refer to our Data Subject Rights policy and procedure for further information including details on how to submit a request and a list of supervisory authorities (details of which are provided in Appendix B).

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 job applicants 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

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