GXO PRIVACY NOTICE FOR EMPLOYEES, WORKERS AND CONTRACTORS

1. PURPOSE

The purpose of this Privacy Notice (the **"Notice"**) is to inform you of GXO's practices regarding the processing of your Personal Data for HR and business purposes, in accordance with Applicable Laws.

In the context of your working relationship with the GXO Group (the **"Company"**, **"we"** or **"us"**), the Company (also known as a **Controller**), will process information about you and your dependents, in both paper and electronic format. We refer to such information as "Personal Data".

This processing may also be carried out by **GXO Logistics, Inc.**, registered at Two American Lane, Greenwich, CT 06831, USA, and other affiliates in the GXO group of companies (collectively, the "**GXO Group**").

If you have any questions regarding which GXO company: (i) you are working for, or (ii) is the Controller of your Personal Data, please contact us (for contact details, see **Section 9** below). The GXO Company which you are working for may be jointly responsible with GXO Logistics, Inc. and its affiliated entities and group companies for the lawfulness of the processing of your Personal Data. We have set out a list of the companies within the GXO Group, which act as Controllers of your Personal Data, at **Annex 2.** The identity of the Controller processing your Personal Data will depend on the location in which you are employed. This Notice may be complemented by additional notices and policies which provide more detailed information about particular processing activities.

In addition to terms defined elsewhere in this Notice, the key terms used in this Notice are defined in **Annex I**.

If you are located in California, please consult the California Privacy Addendum at **Annex 3**.

2. WHAT PERSONAL DATA DO WE COLLECT AND PROCESS?

GXO processes different categories of Personal Data about you, for the purposes described in **Section 3** and in connection with the processing operations in **Section 4** (the categories, purposes and processing operations outlined here may vary, depending on the Applicable Laws and local operational requirements in force in the country in which you are employed). These categories of Personal Data include the following:

2.1 Ordinary Personal Data

- **Identification data**: Including civil/marital status, first and last name, date and place of birth, nationality, gender, photograph, employee ID;
- **National identifiers**: Including national identification or passport number; driver's license; social security number (as may be appropriate and permitted by Applicable Laws and except where prohibited by Applicable Laws), work permit;
- **Contact details**: Including postal or email address, telephone number (fixed and mobile), fax numbers (both business and private);
- **Family members', dependents' and beneficiaries' and emergency contact data**: Including name, address, date and place of birth, telephone number, age and number of children;

- **Academic and professional qualifications**: Including degrees, titles, skills, language proficiency, training information, employment history, CV/resume, past employment references;
- **Information gathered as part of routine identification and background checks** (as may be appropriate and permitted by Applicable Laws and except where prohibited by Applicable Laws): Including gathered in connection with Right to Work checks and identity checks;
- **Financial details**: Including bank account number, bank details, salary and compensation/benefits data, social security and tax information, bonuses, pension qualification information, travelling expenses;
- **Employment data**: Including job title, function, level, supervisor and other job relationships, grade, business unit, department, dates and conditions of employment, working hours, reports and investigation results, disciplinary sanctions; performance review and job appraisals, dates and results of tests and training, promotions, succession/career planning, changes in role, absence records (holiday and other);
- **diversity and inclusion data**: Including first and second languages spoken, information concerning whether you are an armed forces veteran or reservist, or spouse or civil partner of an armed forces veteran or services person, homelessness;
- **IT related data**: Including computer ID, user ID and password, domain name, IP address, log files, your use of the internet, e-mail, and IT systems and applications (including a "risk score" based on data collected about such use);
- **Video data**: Including CCTV footage, dash cam and other recordings and other information from electronic systems
- **Vehicle geolocation data**: Including real-time vehicle location, routes taken, parking locations, GPS coordinates, telematics data, and other location-related data generated through our fleet management systems;
- **Communication data**: Including email and electronic messages, voicemail, files and other correspondence material transmitted using systems of the Company or for Company purposes and stored on servers or Company or on the Company's behalf (as may be appropriate and permitted by Applicable Laws and except where prohibited by Applicable Laws);
- **Personal characteristics**: Including hobbies, interests (as you may have defined on your CV for example); and

- **Operational data:** including data relating to attendance, productivity, work performance, task completion, system utilisation, operational efficiency, and related metrics collected through warehouse management systems and other business operations platforms,

(together, the "**Ordinary Personal Data**").

2.2 Special Categories of Personal Data

Some of the Personal Data that we process are deemed **sensitive** and are referred to as "**Special Categories of Personal Data**" (as defined below), and include:

- where necessary and authorised by Applicable Laws, data relating to your health, including short and long-term disability, and medical care, as well as to your trade union membership or religion (for example, for tax law compliance or to accommodate religious holidays);

- data concerning your nationality, gender, and civil/marital status (for example, to identify you and establish your employee profile);
- your fingerprint data (which is biometric data where it is used for the purposes of uniquely identifying you);
- in relation to our monitoring of equality, diversity and inclusion. For the UK, and the US, the following will be processed: ethnicity, marital status or civil partnership, religion (UK only), sexual orientation, disability or long-term condition, gender, caring responsibilities, long term periods of absence or leave. These particular categories of data are collected only if you choose to provide it to us, and we will only process it with your consent.

We also process data relating to driving offences, information contained in whistleblowing reports and misconduct which may amount to criminal behaviour or criminal offences for HR and administrative as well as compliance purposes, as may be appropriate and permitted by Applicable Laws.

2.3 Sources of the Personal Data

Personal Data Directly from You: We collect Personal Data directly from you (electronically, in writing, or verbally). We may, for example, ask you for information when you begin your employment with the Company. You may also provide new, updated or corrected data to the Company from time-to-time.

Personal Data That We Generate: We may also receive Personal Data from your colleagues or supervisors, for example, from sources generated by us in the normal course of your work, such as in connection with technology and surveillance systems we have in place, annual job performance reviews, pay rise history, disciplinary action, and promotion history. Information on your use of the internet, e-mail, Company systems and applications is automatically generated.

Personal Data from Third Parties: We may also receive Personal Data from third parties who provide services to the Company, such as companies that provide benefits including share option/equity awards, payroll, corporate purchasing cards, or other services. For example, if you have been hired through a third-party staffing or recruiting firm, we will receive personal details and information on your experience and qualifications from them. Where permitted or otherwise authorised by law, information received from third parties may include the results of background checks.

3. FOR WHICH PURPOSES AND ON WHICH LEGAL BASES DO WE PROCESS YOUR PERSONAL DATA

We process Personal Data (which, as set out above at **Section 2**, includes the Ordinary Personal Data and Special Categories of Personal Data) for the following purposes. For each purpose, the legal basis of the processing is specified, in accordance with Articles 6 and 9 of the GDPR (or UK GDPR and any substantial public interest condition under the Data Protection Act 2018), as appropriate. Where you are located in a country which requires you to provide consent to processing (for example, Canada or Singapore), we will obtain your consent prior to processing your Personal Data in accordance with this Notice and Applicable Laws.

Please note that where we have indicated below that our processing of your Personal Data is either:

- necessary for us to comply with a legal obligation; or
- necessary for us to take steps, at your request, to potentially enter into an employment contract with you, or to perform it,

and you choose not to provide the relevant Personal Data to us, we may not be able to enter into or continue our contract of employment or engagement with you.

We use artificial intelligence within certain of our HR systems and IT monitoring processes, including in relation to generating "risk scores" assigned to employees based on their use of the internet, e-mail, and IT systems and applications. However, we always ensure that there is a human involved to review the results produced by these systems and processes, which means that no fully automated decision making occurs.

3.1 HR Management and Administration

We process Ordinary Personal Data to establish, administer and perform the employment contract between you and us, or to manage the working relationship between you and us; for appointments and approvals; to recruit you and to determine eligibility for initial employment (including the verification of references and qualifications); to manage working time and absences; to assess qualifications for a particular job or task; to administer payroll and healthcare and other benefits and equity-related awards; to conduct performance reviews and determine performance requirements; to manage talent; to ensure employee satisfaction; to provide training and learning services (and to identify the need for additional training, where required); to monitor employees' performance and efficiency within our warehouses; to ensure employee safety and ensure efficient allocation of routes and driver activity; for disciplinary matters; to manage accidents and incidents at work; for the purposes of monitoring equality, diversity and inclusion, where authorised by Applicable Laws; to manage legal or other disputes involving you, other workers or contractors or customers (or other individuals/members of the public); or to ensure that we comply with all applicable pay and business reporting requirements to which we may be subject (where authorised by Applicable Laws).

Legal Basis under Article 6 GDPR/UK GDPR. This processing is justified based on:

- the necessity for the performance of the employment contract;
- our legitimate interests in ensuring that we can effectively operate our business from a HR and administration, management, performance and development, health, safety and security and compliance perspective; or
- the necessity to comply with legal obligations, such as those arising under tax, employment, pensions, national implementing legislation, and other Applicable Laws and regulations.

We process the Special Categories of Personal Data and data related to suspected compliance violations to comply with legal and statutory requirements (for example, to confirm whether an employee is fit or not to perform his/her role or as part of our annual or new starter examination or in order to allow the employees to discount their membership

for trade union membership in the payroll); for the purposes of monitoring equality, diversity and inclusion (in the UK and in other jurisdictions, in accordance with Applicable Laws), where authorised by Applicable Laws, and for compliance with all applicable pay and business reporting requirements to which we may be subject (where authorised by Applicable Laws).

This processing is justified based on:

- your explicit consent;
- the necessity for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law;
- the necessity to protect the vital interests of Data Subjects and/or other persons where the Data Subject is physically or legally incapable of giving consent; and/or
- the necessity for the establishment, exercise or defence of legal claims.

3.2 Business Operations

We process Personal Data to manage our projects, orders and accounts, work organisation, provide, supply or acquire products and services, product management, business development, and customer relationship management, employee travel, expense tracking and reimbursement, to ensure that we can properly manage our fleet of vehicles and optimise routes and vehicle utilisation, management reporting and analysis, to conduct financial planning, to determine and review salaries; to measure efficiency and facilitate performance monitoring, and to facilitate employee career development and talent management.

Legal Basis. This processing is justified based on:

- your consent (where required under Applicable Laws).;
- the necessity for the performance of the employment contract;
- the necessity for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law (where Special Categories of Personal Data are involved);
- reasons of substantial public interest (with a basis in law) (where Special Categories of Personal Data are involved); or
- our legitimate interests in ensuring that we can operate our business in the most efficient way possible, and ensuring that we can effectively administer and execute GXO projects, operations and workflows.

3.3 Physical and Network Security, Communications and IT

We process Personal Data to manage and maintain the functioning and security of our IT systems, applications and network; to enable internal contacts and communication; to protect our intellectual property, trade or business secrets and company-held information; to provide IT support and training to employees, including identifying a need for additional training for members of staff on IT security; to monitor employees' use of the internet, e-mail, and IT systems and applications, using an artificial intelligence tool and to analyse

"risk scores" assigned to employees based on that tool's output, and to ensure the safety of our employees, visitors and clients when they are on our business premises and/or use GXO vehicles and to support investigations and detect crime.

Legal Basis. This processing is justified based on:

- our legitimate interests in ensuring that we: (i) maintain a safe, secure working environment, (ii) maintain the security of our IT systems and networks, (iii) can assure employees' compliance with internal policies, and (iv) are equipped to protect our sensitive and proprietary business information;
- your consent (where required under Applicable Laws).

3.4 Compliance

We process Personal Data to ensure compliance with GXO policies and applicable legal and other statutory obligations and for the purpose of facilitating audits, investigations, enquiries, allegations of employee misconduct or criminal behaviour, and for the purposes of conducting disciplinary and performance investigations and procedures, protecting our property and assets, and for the investigation, prevention and detection of crime.

Legal Basis. This processing is justified based on:

- The necessity for the establishment, exercise or defence of legal claims (where Special Categories of Personal Data are involved);
- our requirement to comply with legal obligations to which we are subject;
- our legitimate interests in ensuring that we conduct our business in accordance with appropriate standards and ensuring that we create a safe working environment for our employees

We will process information on criminal behaviour only to the extent permitted by Applicable Laws.

3.5 Sale of Group Companies or businesses

We process Personal Data for the purpose of the sale of GXO Group Companies or businesses in accordance with Applicable Laws.

Legal Basis. This processing is justified based on:

- The necessity for the establishment, exercise or defence of legal claims (where Special Categories of Personal Data are involved);
- The necessity for the performance of a contract;
- The necessity for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social data protection law (where Special Categories of Personal Data are involved); and
- our legitimate interests in ensuring that we can enter into and engage in negotiations, and contractual arrangements which align with our business requirements and objectives.

4. PROCESSING OPERATIONS

Further to the above legal bases which we rely on in order to process your Personal Data, when "processing" your Personal Data, in connection with each of the purposes outlined above, this means that, at the outset of our relationship, and on an ongoing basis, we:

- **collect and record personal data** - this enables us to perform activities such as setting up your employee file, granting you access to internal systems and services, ensuring that employment records remain accurate and up to date, etc;

- **store and delete personal data** – in addition to the above activities, this also enables us to perform activities such as communicating with you throughout the course of your employment relationship with us, handling any questions, or issues, you may have as they arise, retaining Personal Data to comply with applicable laws to which we are subject, and deleting any Personal Data we process on your request, or in accordance with the terms of this Notice (see **Section 8** below); and

- **transmit personal data** – this enables us to perform activities such as transmitting Personal Data to relevant GXO Group companies, conducting relevant regulatory reporting (e.g., pay transparency reporting), and facilitating responses to queries from government agencies (e.g., tax authorities, etc.).

5. WITH WHOM DO WE SHARE YOUR PERSONAL DATA

If necessary for the purposes specified in **Section 3** of this Notice we may share your Personal Data with:

- other GXO Group companies, who need your Personal Data, for example, to provide centralized services to us,

- service providers and business partners, who need your Personal Data to provide their services to us, in particular

    - administration services (e.g. document service providers, facility management, maintenance and repair service providers or security companies),

    - customer service and support services (e.g. call centre, help desk or customer relationship management providers),

    - finance and accounting services (e.g. accountants, banks, credit check agencies, insurers, payment processors, payroll service providers or tax advisors),

    - human resources services (e.g. recruiting agencies, background check providers, trainers, benefit providers, employee survey providers, health and safety providers, including company doctors, travel agencies, accommodation and transport providers),

    - IT and telecommunications services (e.g. cloud service providers, cybersecurity providers, data hosting centres, software providers, IT

maintenance and support providers, electronic communication services providers, or network operators),

- legal and compliance services (e.g. auditors, lawyers, operators of whistleblowing hotlines or other experts),
- marketing and sales services (e.g. marketing and advertising, social media platforms or other media companies),
- strategy and business development services (e.g. management consultants, business intelligence providers or other advisors),

- government authorities, who need your Personal Data to perform their public tasks (e.g. courts for litigation, tax authorities for tax administration or law enforcement authorities for investigations), or

- other parties, such as our customers, potential buyers of our business (e.g. in case of a sale, merger, or acquisition), counterparties including their service providers (e.g. in litigation), or other recipients at your direction.

GXO takes care when sharing Personal Data with other internal (i.e., intra-group) or external parties. In particular, any service providers and business partners engaged by GXO will have access to Personal Data solely to the extent necessary to enable them to perform services on GXO's behalf and GXO will endeavour to ensure that they are contractually prohibited from using Personal Data for any other purpose. GXO will obtain assurances from these recipients that they will safeguard Personal Data consistently with this Notice.

6. INTERNATIONAL TRANSFER OF PERSONAL DATA

Given that GXO Group companies are located and provide services all over the world, we need to transfer your Personal Data internationally, including outside your jurisdiction of residence. If we transfer your Personal Data to recipients in countries outside of the EEA (i.e. a Third Country), we apply the following transfer safeguards to ensure the protection of your Personal Data:

- For recipients in Third Countries with an adequate level of protection, such as Canada or Switzerland, we rely on the EU Commission's adequacy decisions (you can find the current list of adequate Third Countries at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

- For recipients in Third Countries without an adequate level of protection, such as India or the US, we usually rely on standard contractual clauses (you can find the text of the standard contractual clauses at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en).

- For recipients in Third Countries without an adequate level of protection and in the absence of standard contractual clauses, we rely on derogations under Art. 49 GDPR, for example, if you have given your explicit consent, it is necessary for the

conclusion or performance of a contract with you or in your interests, or it is necessary to establish, exercise, or defend legal claims.

The data protection laws of those other countries might be different from the laws of your jurisdiction, and might permit the government, government agencies, courts, law enforcement agencies and security authorities in those countries to access your personal information without notice.

Please write to privacy@gxo.com if you want to receive further information or, where available, a copy of the relevant data transfer mechanism.

7. HOW LONG WE KEEP YOUR PERSONAL DATA

We keep your Personal Data for no longer than is reasonably necessary for the purpose for which it was collected, being specified in our GXO Group records retention policies (if you are located in one of the Member States of the European Union, (you can find our Data Retention Policy at https://ethics.gxo.com/) . To determine our retention periods, we particularly use the following criteria:

- If you withdraw your consent or object to the processing of your personal data and we cannot rely on another legal basis, we will usually not store your personal data for any longer;
- If we are legally obliged to retain your personal data (e.g. for tax purposes), we will usually store your personal data for the prescribed retention period;
- If we are legally obliged to delete your personal data, we will usually not store your personal data for any longer;
- If we need your personal data to establish, exercise, or defend legal claims, we will usually store your personal data for the statutory limitation period or until legal proceedings are concluded;
- If we have an existing relationship with you, we will usually store your personal data for the period of our relationship;
- If we likely need to use your personal data in the future, we will usually store your personal data for this anticipated period in the future.

We also implement appropriate technical, physical and organisational measures to ensure that Personal Data is kept secure and protected from loss, misuse and unauthorised access or disclosure. Once our applicable storage periods expire, we will securely delete or anonymize your personal data in accordance with applicable laws requirements.

If you have further questions regarding our retention of your Personal Data, you can contact us (see **Section 9** below).

8. YOUR RIGHTS WITH RESPECT TO YOUR PERSONAL DATA

In relation to the processing of your personal information by GXO, you may have the following rights (depending on the jurisdiction in which you are located):

8.1 Request Access to Your Personal Data

You have the right to obtain confirmation from us as to whether or not your Personal Data are being processed, and related information, and to obtain a copy of your Personal Data undergoing processing subject to applicable exemptions under Applicable Laws.

8.2 Request Rectification of your Personal Data

In certain jurisdictions, you have the right the request that we rectify (i.e., correct) any inaccurate Personal Data, and to have incomplete Personal Data completed.

8.3 Objection to Processing

In certain jurisdictions, you have the right to object to the processing of your Personal Data on grounds relating to your particular situation. For example, this right applies where: your Personal Data is processed in accordance with the legal basis of legitimate interests (including where profiling is carried out on that basis). In such a case we shall no longer process the Personal Data unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant Data Subject(s) or for the establishment, exercise or defence of legal claim.

8.4 Request the Portability of your Personal Data

In certain jurisdictions, you may receive your Personal Data that you have provided to us in a structured, commonly used and machine-readable format and have the right to transmit it to other controllers without hindrance. This right only exists if the processing is based on your consent or a contract, and the processing is carried out by automated means.

8.5 Request Restriction of Processing of your Personal Data

In certain jurisdictions, you may request to restrict processing of your Personal Data (in certain cases permitted under the Applicable Laws). This enables you to ask us to suspend the processing of your Personal Data, for example, if you want us to establish its accuracy.

8.6 Request Erasure of your Personal Data

In certain jurisdictions, you may request us to erase your Personal Data, and we will do so (unless there is a good reason for us to continue to process it). In these cases, we will delete, destroy or anonymize the Personal Data in accordance with applicable laws requirements.

8.7 Right to lodge a complaint

You also have the right to lodge a complaint with a Supervisory Authority, in particular in the EU Member State or country of your residence, place of employment, or the location where the issue that is the subject of the complaint occurred.

8.8 Right to refuse or withdraw consent

In a situation where we have asked for your consent to processing, you are free to refuse to give consent and you can withdraw your consent at any time. Please keep in mind that withdrawing your consent does not have retroactive effect. This means that the withdrawal does not affect the lawfulness of past processing based on consent before its withdrawal.

The Company is therefore not required to undo any past processing following the withdrawal of your consent.

8.9 Right to make a data protection complaint (UK GXO entity only)

You have the right to make a data protection complaint directly to the GXO UK entity where you consider the GXO UK entity has infringed the UK data protection laws. You can do this prior to complaining to the Supervisory Authority in the UK, the Information Commission.

9. CONTACT

If you wish to exercise any of the afore-mentioned rights (see **Section 8**) or if you have any questions regarding this Notice or other questions, comments or concerns about our privacy practices, please contact your local HR manager, or the Privacy Office at privacy@gxo.com.

In the event that you experience any incident, or breach involving your Personal Data, or the Personal Data of any other individual, please report it to us immediately at privacy@gxo.com.

You can also contact the data protection officer, if appointed in your country (see Annex 2 for details).

10. UPDATES TO THIS NOTICE

GXO may from time to time make changes to this Notice to reflect changes in our legal or regulatory obligations. We will communicate any revised version of this Notice by posting it on the company intranet site and through other suitable means of communications.

This Notice was last updated on 1st October 2026.

Annex I: Definitions

Company	means the GXO legal entity that employs you.
Controller	means, for the purposes of this Notice, the GXO entity that determines the purposes and the means of the processing of the Personal Data. A list of Controllers is set out at **Annex 2** of this Notice.
Applicable Laws	refers to all relevant and applicable laws and regulations in effect in the country in which the relevant Data Subject is located, including without limitation: (i) all privacy and data protection laws, statutes, directives, regulations, decrees, and other legislative measures or decisions having effect in any jurisdiction from time to time, including the EU General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**") (and all national implementing laws); (ii) the UK Data Protection Act 2018 and the General Data Protection Regulation (Regulation (EU) 2016/679) as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**"); and (iii) the Singapore Personal Data Protection Act of 2012.
Data Subject	means the natural person to whom the Personal Data relates.
European Economic Area or EEA	means the 27 Member States as well as Norway, Iceland and Liechtenstein.
employees	includes full-time employees, part-time employees, temporary employees, reinstated employees, rehired employees and retired and former employees.
Member States	means the 27 member states of the European Union, as follows: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

Personal Data	More generally, personal data is information relating to an identified or identifiable natural person. 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.
processing or processed	means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller
Special Categories of Personal Data	is a subset of a Personal Data that is 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 the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Whilst not Special Categories of Personal Data, personal data relating to criminal convictions and offences or related security measures are also sensitive data.
Third Country	means a country outside the EEA.
Third Party	means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.
Supervisory Authority	means any governmental or regulatory authority, responsible for enforcing any of the relevant Applicable Laws, and any replacement or successor body or person for any such authority from time to time.

Annex 2

List of GXO legal entities which currently act as Controllers

[TBC]

Scope	Identity and contact details
	Controller: **[If applicable] Data protection officer**: [Email address]

Annex 3
CALIFORNIA EMPLOYEE PRIVACY ADDENDUM

Effective Date: 1st October 2026

1. Overview

This addendum to the employee privacy notice ("**California Privacy Addendum**") applies to the collection and use of personal information (defined below) in the context of a California resident's role as an employee ("**you**", or "**your**") by **GXO Logistics, Inc.** and affiliates (collectively, "**GXO**," "**we**," "**us**," or "**our**"). **This California Privacy Addendum only applies and the rights herein are restricted to California residents, unless otherwise required by applicable law.**

In this context, **personal information** generally means information that is defined as personal data, or identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with you or your household (e.g. your name, telephone number, Employee ID number, or information defined as personal information under California privacy laws)[1].

Processing means any activity relating to personal information, including, by way of example, collection, storage, use, consultation, disclosure, sharing and transmission.

In summary, we collect and process personal information about you in order to hire or engage you, pay you, provide you with and administer benefits (to the extent applicable), to pay taxes (to the extent applicable), and to ensure your safety and well-being.

This California Privacy Addendum is not an employment contract. If you are an employee, employment with GXO is on an "at-will" basis, meaning that either you or GXO may terminate your employment at any time, with or without cause or notice.

2. What types of personal information do we collect and where do we get it from?

Your personal information that we collect may include the categories set forth in the chart below, in accordance with the principles outlined in this California Privacy Addendum. **These categories and the definitions set forth in the table below are as defined by California's privacy laws.**

These categories also represent the categories of personal information that we have collected over the past 12 months and shared with our service providers and affiliates. Note that the categories listed below are defined by California state law. Inclusion of a category in the list below indicates only that we may collect some information within that category. It does not necessarily mean that we collect all information listed in a particular category. *Information denoted with an * indicates sensitive personal information, which is further discussed in Paragraph 3.*

[1] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et. seq., including as amended by the California Privacy Rights Act of 2020, and all regulations issued thereunder.

Category of personal information collected	Categories of sources from which personal information is collected	Purpose of collecting/processing
Personal identifiers. Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number*, driver's license number*, passport number*, or other similar identifiers.	• You (directly or indirectly). • Third party service providers (e.g., benefits providers). • Government agencies and actors, and/or other third parties (e.g., former employers). • Publicly available job or networking sites on which you post this information.	To administer your relationship with us, including meeting our legal obligations and providing you with benefits and services, as applicable.
Information About You. Information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, your name, signature, social security number*, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number*, insurance notice number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.		

Category of personal information collected	Categories of sources from which personal information is collected	Purpose of collecting/processing
Characteristics of classes protected under federal or California law, including: familial status, disability, sex, national origin, religion, color, race, sexual orientation, gender identity and gender expression, marital status, veteran status, medical condition, ancestry, source of income, age, or genetic information.		To administer your relationship with us, including meeting our legal obligations, demonstrating the organization's diversity and inclusion, and providing you with benefits and services, as applicable.
Usage Information. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet web site, application, or advertisement.	• You, typically through your use of cookies and similar technologies. • Your interaction with GXO's devices and equipment.	To administer your relationship with us, including meeting our legal and compliance obligations and pursuing the efficient management and operation of our business, quality control and training purposes, manage productivity, to help detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and for compliance management.
Geolocation information.	• Your interaction with GXO's devices and equipment.	
Recordings. Audio, electronic, visual, thermal, olfactory, or similar information.	• Internal and external CCTVs and geolocation monitors/devices • Recording of customer service and/or sales calls. • Your interaction with GXO's devices and equipment.	

Category of personal information collected	Categories of sources from which personal information is collected	Purpose of collecting/processing
Professional or employment-related information.	• You (directly or indirectly). • Third party service providers (e.g., benefits providers). • Government agencies and actors, and/or other third parties (e.g., former employers). • Publicly available job or networking sites on which you post this information.	To administer your relationship with us, verify credentials, and to pursue the efficient management of our business.
Inferences drawn from other personal information: Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	• You, typically through the use of online assessments. • Publicly available job or networking sites.	To administer your relationship with us, including training and coaching purposes, to operate our business, and in order to help detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and for compliance management.
Biometric information.*[2]	• Your interaction with equipment and/or mobile devices owned or managed by GXO or by our service providers under our instructions.	To help detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and for compliance management.

3. Sensitive Personal Information

We do not use or disclose sensitive personal information we collect for purposes other than those generally permitted under California law, including as needed to perform our services, verify and maintain the quality and safety of our services, and resist fraud or illegal actions. Your sensitive personal information that we collect may include the categories set forth in the chart below, in accordance with the principles outlined in this California Privacy Addendum. **These categories and the definitions set forth in the table below are as defined by California's privacy laws.**

[2] This includes physiological, biological or behavioral characteristics that can be used, singly or in combination with each other or with other identifying information, to establish individual identity.

Category of sensitive personal information collected	Categories of sources from which sensitive personal information is collected	Purpose of collecting/processing
Social security number, driver's license number or other state ID number, and passport information.	• You (directly or indirectly). • Third party service providers (e.g., benefits providers). • Government agencies and actors, and/or other third parties (e.g., former employers). • Publicly available job or networking sites on which you post this information.	Social security number - to administer your relationship with us, particularly as it relates to taxation and background checks. Passport information - to verify your right to work, and it may be used to book travel for you or for other legal/regulatory obligations. Driver's license number or other state ID – to verify identity as required under applicable laws, and if driving is a requisite for performance of your job duties, to ensure your suitability to drive and for insurance purposes.
Racial or ethnic origin, and religious or philosophical beliefs.		To administer your relationship with us, demonstrating the organization's diversity and inclusion, and to meet our legal obligations.
Precise geolocation	Your interaction with equipment and/or mobile devices owned or managed by GXO or by our service providers under our instructions.	To help detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and for compliance management. To administer your relationship with us and to operate our business.
Health Information i.e., personal information collected and analyzed concerning your health.	• You (directly or indirectly). • Third party service providers (e.g., benefits providers).	To manage our workforce, including to ascertain whether you may have been exposed to a virus in connection with a pandemic.

Category of sensitive personal information collected	Categories of sources from which sensitive personal information is collected	Purpose of collecting/processing
Mail, email, and text messages contents (except where we are the intended recipient of the communication).	Your interaction with equipment and/or mobile devices owned or managed by GXO or by our service providers under our instructions.	To administer your relationship with us, including performance management, and in order to help detect security incidents, and for compliance management.
Genetic data.	• You (directly or indirectly). • Third party service providers (e.g., benefits providers).	To provide you with benefits and services, as applicable.
Personal information collected and analyzed concerning your sexual orientation.		
Biometric information[3]	Your interaction with equipment and/or mobile devices owned or managed by GXO or by our service providers under our instructions.	To help detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, and for compliance management. To administer your relationship with us and to operate our business.

4. How we process your personal information

As noted in the above tables, we process personal information about you, in accordance with applicable law and this California Privacy Addendum, for the purposes of administering your relationship with us, administering our workforce generally, and running our business operations. Processing for these general purposes includes, but is not limited to, processing for the specific purposes as provided in the privacy notice.

The broad classes of third parties to which we may transfer personal information about you have been set forth in the privacy notice.

[3] This includes physiological, biological or behavioral characteristics that can be used, singly or in combination with each other or with other identifying information, to establish individual identity.

We do not and do not intend to "sell" personal information about you or "share" it for cross-context behavioral advertising, as defined under applicable privacy law. We also have not done so for the last 12 months. In addition, we do not share the personal information with third parties for their direct marketing or advertising purposes.

For purposes of this California Privacy Addendum, "sold" means the disclosure of personal information for monetary or other valuable consideration and "cross-context behavioral advertising" means targeted advertising based on personal information obtained from your activity across businesses, distinctly-branded websites, applications, or services, other than our websites and services with which you intentionally interact.

We will endeavor to ensure that all non-governmental third parties to which we transfer personal information about you agree, as part of their contract with us, to treat personal information about you in accordance with applicable privacy laws.

5. Your Privacy Rights

- *Right to Know* – You may be entitled to request that we disclose to you personal information we have collected about you, the categories of sources from which we collected the information, the purposes of collecting the information, the categories of third parties with whom we have shared the information, the categories of personal information that we have shared with third parties for a business purpose, the categories of information sold, and the categories of third parties information is sold to. In some instances, you may have the right to receive the information about you in a portable and readily usable format. Before providing any of this information, we must be able to verify your identity.
- *Right to Opt-Out* – You may have the right to opt-out of information sharing that constitutes "selling" or "sharing" personal information under California law.
- *Right to Limit* –You may have the right to direct us to limit our use of your sensitive personal information to certain purposes.
- *Right to Deletion* – Subject to certain conditions, you may be entitled to request that we delete personal information about you. Before deleting personal information, we must be able to verify your identity. We will not delete personal information about you when the information is required to fulfill a legal obligation, is necessary to exercise or defend legal claims, or where we are required or permitted to retain the information by law. For example, we cannot delete certain personal information about you while continuing to provide you with certain products and services or where we are legally required to retain certain information.
- *Right to Correction* – You may be entitled to request that we correct inaccurate personal information. Before collecting personal information, we must be able to verify your identity. We will not correct personal information about you when the information is required to fulfill a legal obligation, is necessary to exercise or defend legal claims, or where we are required or permitted to retain the information as-is by law.

Data solely retained for data backup purposes is principally excluded from these rights until it is restored to an active system or next accessed or used for a sale, disclosure, or commercial purpose.

If you chose to exercise any of these rights, to the extent that they apply, privacy law prohibits us from discriminating or retaliating against you on the basis of choosing to exercise your privacy rights.

Please note that under applicable privacy law, we are only obligated to respond to personal information requests from the same California resident up to two times in a 12-month period. In addition, under applicable privacy law, and for the protection of your personal information, we may be limited in what personal information we can disclose.

Before providing information you request in accordance with these rights, we must be able to verify your identity. In order to verify your identity, you will need to submit information about yourself, including your name, contact information, and proof of identity. We will match this information against information we have previously collected about you or provided to you to verify your identity

and your request. If we are unable to verify your identity as part of your request, we will not be able to satisfy your request. We are not obligated to collect additional information in order to enable you to verify your identity. For deletion requests, you will be required to submit a verifiable request for deletion and then confirm separately that you want personal information about you deleted.[4]

Information collected for purposes of verifying your request will only be used for verification. **You can submit requests related to your personal information by submitting your request to privacy@gxo.com**

6. Changes to this California Privacy Addendum

We may change this California Privacy Addendum at any time. The California Privacy Addendum, and any updates to the California Privacy Addendum, will be posted on https://ethics.gxo.com/ . You may visit https://ethics.gxo.com/ to view the most current version of the California Privacy Addendum. The date the California Privacy Addendum was last revised will appear at the top of the page as the effective date.

7. Contact Details

If you have any questions, concerns, complaints or suggestions regarding our California Privacy Addendum or the personal information collected about you, please contact us via email at privacy@gxo.com or contact GXO Logistics, Inc, Two American Lane Greenwich, CT 06831.

[4] If you would like to appoint an authorized agent to make a request on your behalf, you must provide the agent with written, signed permission to submit privacy right requests on your behalf. Alternatively, your authorized agent may provide evidence of having power of attorney or acting as a conservator for you.