GXO

GXO Privacy Policy

Contents

This Policy is owned and maintained by – The Ethics and Compliance Office – ethics@gxo.com

1. Introduction

This Privacy Policy is supplemental to the **GXO Logistics, Inc**. "**Business Ethics Policy – Data Protection**". It applies to GXO Logistics, Inc., including all of its subsidiaries, divisions and other operating entities (collectively, "GXO", "We" or "the Company"). All directors, officers and employees of GXO, and third parties acting on our behalf, are subject to and responsible for complying with these requirements of this policy.

2. Definitions

The words or abbreviations used in this Policy will have the meaning given to them in the table below.

Automated Decision-Making (ADM)	When a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing
Automated Processing	Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Company Personnel	All employees, workers, contractors, agency workers, consultants, directors, members and others.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.
Data Controller	The person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. GXO is the Data Controller of all Personal Data relating to GXO Personnel and Personal Data used by GXO for its commercial purposes.
Data Subject	A living, identified or identifiable individual about whom We hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.
Data Privacy Impact Assessment (DPIA)	Tools and assessments used to identify and reduce risks of a data processing activity.
EEA:	The 28 countries in the EU, and Iceland, Liechtenstein and Norway
General Data Protection Regulation (GDPR):	The General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.
Personal Data:	Any information identifying a Data Subject or information relating to a Data Subject that We can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach	Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that We or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR
Privacy Notices (also referred to as Fair Processing Notices)	Separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose
Processing or Process	Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties
Pseudonymisation or Pseudonymised	Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure
Sensitive Personal Data:	Information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

3. Scope

This Privacy Policy sets out how GXO collects and maintains the Personal Data of our employees, workers, customers, suppliers, and other third parties.

This Policy is developed in compliance with the General Data Protection Regulation (EU) 2016/679 (“GDPR”) and applies to all Personal Data (meaning information relating to or which identifies living individual persons) where the Personal Data is being Processed by;

- legal entities or enterprises located in the EU even if the processing takes place outside of the EU; and
- enterprises or legal entities located outside of the EU when such enterprise or legal entities market goods or services to individuals in the EU or engage in monitoring activities of individuals’ behaviour in the EU.

It applies to GXO’s activities in relation to its EU employees, potential employees, customers, suppliers and other third parties in connection with whom GXO Processes Personal Data.

To the extent that that this Policy differs from or has more stringent requirements than the GXO Logistics, Inc., Business Ethics Policy – Data Protection, then this Policy and the requirements of the GDPR will prevail.

4. Responsibility

Proper data management is critical to maintaining the trust of all those with whom We do business. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that We take seriously at all times.

All directors, officers and employees of GXO, and third parties acting on our behalf are responsible for complying with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Chief Compliance Officer is responsible for overseeing this Privacy Policy and developing related policies and Privacy Guidelines and may be contacted via;

ethics@gxo.com

The Chief Compliance Officer is supported in these activities by the Privacy Office. This can be contacted at;

gdpr@gxo.com

Each country/Business unit has a designated Privacy Officer. This will be identified to you by your local HR Business Partner.

Please contact the Privacy Office or your local Privacy Officer if you have questions or concerns about managing Personal Data or compliance with GDPR.

You must always contact the Privacy Office and your local Privacy Officer if you believe that there has been a Personal Data breach (see section 8.2) or if you have received a request from a Data Subject to exercise their rights (see section 7) and for the other matters listed at **Appendix 1.**

5. Personal Data Protection Principles

We must comply with the Personal Data Protection Principles when Processing Personal Data. The Principles are :

5.1. Lawfulness, Fairness and Transparency

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

5.2. Lawfulness and Fairness:

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent Processing, but ensure that We Process Personal Data fairly and without adversely affecting the Data Subject.

You may only Process Data if it is for one of the lawful purposes. **These are listed at Appendix 2.**

Where Consent of the Data Subject is the lawful basis for Processing, this consent must be explicit, meaning that Data Subjects must clearly indicate their agreement by a statement or ticking a box. Pre-ticked boxes, silence or inactivity are not confirmation of consent by a Data Subject.

5.3. Transparency (Notifying Data Subjects):

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects (whether the information was collected directly from Data Subjects or from elsewhere) about;

- Who is the Data Controller;
- What Personal Data is collected;
- How and why it will be processed;
- Who it will be disclosed to;
- How we will protect it; and
- How long we will retain it.

Such information must be provided through appropriate Privacy Notices.

We must provide this information through Privacy Notices which must be presented when the Data Subject first provides the Personal Data. The Notices must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

This includes the Personal Data that We collect for human resources and employment purposes.

5.4. Purpose Limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

5.5. Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only collect Personal Data that you require for your job duties: do not collect excessive data.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with any applicable laws or guidelines.

5.6. Accuracy

Personal Data must be accurate and kept up to date. It must be corrected or deleted without delay when inaccurate. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

5.7. Storage Limitation.

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

5.8. Data Subject's Rights and Requests.

Personal data must be made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data. (See Section 7 below).

5.9. Security, Integrity and Confidentiality.

Personal Data must be Processed in a manner that ensures its security by using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage. (See Section 8 below).

5.10. Transfer Limitation.

Personal Data must not be transferred to another country without appropriate safeguards being in place. (See Section 10 below).

6. Record of Processing

The GDPR requires us to keep full and accurate records of all our Data Processing activities. You are responsible for ensuring that correct corporate records are maintained reflecting our Processing in accordance with the Company's record keeping guidelines.

These records should include, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

These Data Processing records are managed by the Privacy Office. However, you are responsible for assisting the Privacy Office as required in creating and maintaining these Data Processing records and you must for inform the Privacy Office of any new Processing activities or changes in Processing activities.

7. Data Subjects Rights and Requests

The individuals whose Personal Data We process are referred to in the GDPR as Data Subjects. Data Subjects have rights regarding how We handle their Personal Data. **These rights are listed in full at Appendix 3**.

If you receive a request from a Data Subject in relation to the processing of their Personal Data, you must follow the Subject Access Procedure and log the request with the Privacy Office and your local Privacy Officer by reporting it at;

gdpr@gxo.com –
Please title your email –**Personal Data Subject Access Request**

The Privacy Office will advise and assist you in relation to responding to the request. Subject data Requests must be responded to **within 30 calendar days**. You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

8. Security

8.1. Technical and Organisational Security Measures

We must implement appropriate technical and organisational measures to ensure that our systems for processing Personal Data are secure and comply with the Data Protection Principles. The level of security required should take into account the state of the art technologies, cost of implementation and the nature, scope, context and purpose of Processing. Such measures may include;

- Anonymisation or pseudonymization and encryption of personal data
- The ability to ensure confidentiality, integrity, availability and resilience of processing systems and services
- Ability to maintain and restore the availability and access to Personal Data
- A process for regularly testing, assessing and evaluating the effectiveness of Personal Data

You must comply with XPO's Information Security Policies in relation to Personal Data.

8.2. Data Breach Reporting

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject **within 72 hours** of becoming aware of the breach.

A Persona Data breach is an act or omission that which results in the loss, or unauthorised access, disclosure or acquisition, of Personal Data.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred;

- Immediately report the breach or suspected breach at gdpr@gxo.com
  Please title your email - **Suspected Personal Data Breach**
- Contact the Privacy Office and your local Privacy Officer.
- Do not attempt to investigate the matter yourself.
- Preserve all evidence relating to the potential Personal Data Breach.

9. Privacy by Design and Data Protection Impact Assessment (DPIA)

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art technology;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data Controllers must also conduct Data Privacy Impact Assessments (DPIA) in respect to high risk Processing and when implementing major system or business change programs involving the Processing of Personal Data. You should contact the Privacy Office in order to determine whether a DPIA is required if you are carrying out these activities.

Details of a DPIA are at Appendix 4.

10. Data Sharing and Transfer Limitations

Personal Data should only be shared with third parties if safeguards and contractual arrangements have been put in place.

10.1. Data Sharing within the XPO Group of Companies

You may only share the Personal Data that We hold with another employee, agent or representative of the GXO Group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information.

For transfers of Personal Data within the GXO Group We have an inter group data sharing agreement that governs these transfers even if they are outside of the EU to GXO companies in the United States of America. If you are asked to transfer information outside of the EU to a country other than the United States of America, you must contact the Privacy Office.

10.2. Data Sharing with Third Parties

You may only share the Personal Data We hold with third parties (outside of GXO), such as our service providers if they have a need to know the information for the purposes of providing the services and have a fully executed written contract that contains GDPR approved third party clauses.

10.3. Data Transfers Outside of the EU

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. A transfer occurs when Personal Data is sent from a country inside the EU to a country which is not part of the EU.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the transfer is to an GXO company in the United States of America and the recipient has a job related need to have the Personal Data, or

(b) the transfer is to a third party and you have confirmation from the Privacy Office that appropriate safeguards are in place and that the Data Subject has provided Consent to the proposed transfer after being informed of any potential risks. Or the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

11. Training and Audit

We are required to ensure all relevant GXO employees have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance. You must complete all mandatory data privacy related training that you are requested to complete.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

12. Outsourcing Services

When We need to outsource services to a third party such as IT service suppliers or engage cloud service suppliers involving the processing of personal data this will trigger data protection considerations. Typically, the service suppliers will act as processors and a written processor agreement needs to be put in place.

13. Automated Processing/Profiling/Decision-Making and Direct Marketing

The GDPR has strict rules around automated processing, decision making and profiling. You may only conduct automated processing activities after consultation with the Privacy Office and the completion of a DPIA.

Similarly there are specific rules around direct marketing. Direct marketing campaigns should only be undertaken after consultation with the Privacy Office and the completion of a DPIA.

14. Changes to this Privacy Standard

We reserve the right to change this Privacy Policy at any time without notice.

This Privacy Policy does not override any applicable national data privacy laws and regulations in countries where the GXO operates and certain countries may have localised variances to this Privacy Standard which are available upon request to the Privacy Office.

This Privacy Standard was last amended 2 August 2021

VERSION CONTROL			
Ver. No.	**Release Date**	**Approved By**	**Reason for New Release**
1	08/02/2021	Chief Compliance Officer	Documentation of existing policy

Appendix 1

You must always contact the Privacy Office in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see *Section 5 and Appendix 2*);

(b) if you need to rely on Consent and/or need to capture Consent (see *Section 5.2 and Appendix 2*);

(c) if you need to draft Privacy Notices (see *Section 5.3*);

(d) if you are unsure about the retention period for the Personal Data being Processed (see *Section 5.7*);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see *Section 8.1* below);

(f) if there has been a Personal Data Breach (*Section 8.2*);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see *Section 10)*;

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see *Section 7 and Appendix 3*);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see *Section 9*) or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see *Section 13*);

(k) If you need help complying with applicable law when carrying out direct marketing activities (see *Section 13*); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see *Section 9* and *Section 12*).

Appendix 2

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless We can rely on another legal basis of Processing, Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Consent.

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices;

Appendix 3

The rights of a Data Subject are:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the relevant Supervisory Authority/ statutory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

Appendix 4

You should contact the Privacy Office to conduct a DPIA (and discuss your findings) when implementing major system or business change programs involving the Processing of Personal Data including:

(a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(b) Automated Processing including profiling and ADM;

(c) large scale Processing of Sensitive Data; and

(d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

You must comply with the Company's processes on DPIA and Privacy by Design.