Business Ethics Policy

Data Protection

GXO

Applicability

This Data Protection Policy ("Policy") applies to GXO Logistics, Inc., including all of its subsidiaries, divisions, and other operating entities (collectively, "GXO" 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 the requirements of this Policy. As used in this Policy, the term "Company" should be read to include all persons and entities subject to this Policy.

1 Overview

GXO collects and maintains Confidential Information, Intellectual Property and Personal Data in the course of its operations. This data is collected from employees, customers, suppliers and other third parties. Proper data management is critical to maintaining the trust of all those with whom we do business. The Company is committed to complying with all applicable data privacy and data protection laws, wherever it does business.

If applicable law differs from or has more stringent requirements than this Policy, applicable law prevails. This Policy is not intended to create any additional rights or obligations other than those existing under applicable law.

2 Definitions

2.1 *The Company:* GXO Logistics in all its business forms, employees of GXO, and all other parties as defined under "Applicability."

2.2 *Confidential Information:* Information, in any form, that is not published or available to the public. Confidential Information may include business plans, customer lists, pricing data, process information or company expertise.

2.3 *Data Subject:* An individual from which Personal Data or other data is collected.

2.4 *Intellectual Property:* Intangible property that is the product of human knowledge. Intellectual Property may be concrete (for example, copyrightable work, protectable trademarks or patentable inventions), or abstract (for example trade secrets or ideas).

2.5 *Personal Data:* Information, in any form, that can be used, on its own or in conjunction with other information, to identify an individual. Depending on the jurisdiction, Personal Data may include names, social security or government issued identification numbers, driver's license or passport numbers, addresses, phone numbers, e-mail addresses, financial account numbers, passwords or PINs, unique biometric or health data, or answers to security questions that would allow access to a person's financial account.

3 Standards of Conduct: Personal Data

3.1 *Collection:* Collection of Personal Data shall be limited to data that is necessary for carrying out the Company's operations and is collected through legitimate, lawful means. The Company shall provide appropriate notice to Data Subjects regarding the purpose for which Personal Data is being collected.

3.2 *Use:* Unless otherwise authorized by law or consented to by the Data Subject, the Company shall limit its use of Personal Data to the purpose for which the Personal Data was collected.

3.3 *Quality and Retention:* The Company shall implement reasonable measures to ensure that all Personal Data collected and stored by the Company is accurate and up-to-date. Personal Data is to be archived, deleted, or destroyed when it is no longer needed for legitimate purposes or required to be maintained by law.

3.4 *Security:* The Company shall utilize reasonable technical and organizational controls to safeguard all Personal Data in its possession from improper disclosure, unauthorized access or use, destruction, or loss.

3.5 *Disclosure:* The Company shall not disclose or share Personal Data with any other person or entity unless disclosure is authorized by law or consented to by the Data Subject.

3.6 *Data Subject Rights:* The Company shall provide Data Subjects with appropriate rights of access, correction and deletion of Personal Data that the Company possesses regarding that Data Subject.

3.7 *Reporting of Data Breaches:* The Company shall report any data breach involving Personal Data to the required parties and within the required time frame, as specified by applicable laws.

4 Standards of Conduct: Confidential Information and Intellectual Property

4.1 *Disclosure:* The Company shall only disclose Confidential Information or Intellectual Property, internally or externally, on a "need-to-know" basis and as necessary for business operations. Such information may only be shared externally when proper protective measures, such as a nondisclosureagreement, are in place.

4.2 *Security:* The Company shall utilize reasonable technical and organizational measures to safeguard all Confidential Information and Intellectual Property from improper disclosure, unauthorized access or use, destruction, or loss.

4.3 *Retention:* Subject to applicable data retention laws, the Company archives, deletes, or destroysConfidential Information that is no longer needed forlegitimate purposes.

4.4 *Continuing Obligation:* All persons subject to this Policy have a continuing obligation not to disclose the Company's Confidential Information and Intellectual Property after leaving the Company.

5 Reporting

All persons subject to this Policy must immediately report actual or suspected data breaches, and/or any misconduct or potential violations of this Policy and/or applicable data privacy laws. GXO does not permit retaliation against any person who, in good faith, reports any concerns, misconduct, and/or potential violations of Company policy or applicable laws.

Reports can be submitted directly to the Ethics and Compliance Office at ethics@gxo.com. Additionally, you can visit our Ethics website at https://ethics.gxo.com where you can find alternative reporting options Your concerns can bereported anonymously, unless otherwise prohibited by applicable local law.

Additional information and guidance regarding this Policy can be obtained from the Ethics and Compliance Office at ethics@gxo.com. Notwithstanding the obligation to protect and not disclose Company confidential or proprietary information stated here and in other GXO policies, an individual will not be held criminally or civilly liable under trade secret laws for the disclosure of trade secrets in confidence to government officials or to an attorney when disclosed solely for the purpose of reporting or participating in the investigation of a suspected violation of law. Further, an employee who files a lawsuit against his or her employer for retaliation against the employee for reporting a suspected violation of law may disclose trade secrets to his or her attorney and in litigation as long as the trade secret information is filed under seal.

6 Policy Exceptions

Any exception to or deviation from this Policy must be approved in writing by the Company's Chief Compliance Officer.

7 Failure to Comply

Failure to comply with this Policy could have seriousconsequences for the Company and the individuals involved, including civil or criminal prosecution, fines and possible imprisonment. Violations of this Policy may also result in serious disciplinary action, including termination of employment.

VERSION CONTROL

Ver. No.	Release Date	Approved By	Reason for New Release

1	08/02/2021	Chief Compliance Officer	Documentation of existing policy