PRIVACY POLICY
(PRIVACY PROTECTION POLICY)

INTRODUCTION

At GXO, we are committed to protecting your privacy and personal data. This Privacy Protection Policy has been developed in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data (hereinafter referred to as the Regulation), as well as other legal requirements of the European Union and the Slovak Republic, industry recommendations, and best practices.

This Privacy Protection Policy explains how we process your personal data, i.e., any information that directly or indirectly relates to you, your rights regarding privacy, and how we protect them.

DEFINITIONS

- Data Subject — A natural person whose personal data is processed.
- Controller — A natural or legal person, public institution, agency, or other body that alone or jointly with others determines the purposes and means of personal data processing; in this case, GXO.
- Personal Data — Any information that relates to a Data Subject, such as name, surname, identification number, address, phone number, email address, financial transactions, and other personal activities.
- Processing of Personal Data — Any operations performed on personal data, such as collecting, recording, organizing, storing, using, disclosing, transmitting, or deleting.

• Consent — A freely and knowingly given agreement by the Data Subject to process their
personal data for a specific purpose.
• Profiling — The use of personal data to evaluate an individual's behavior, including financial
activity, preferences, interests, and risks.
• Processor — A person or entity that processes personal data on behalf of the Controller.
• Third Party — A person or entity other than the Data Subject, Controller, or Processor who is
authorized to process personal data under the direct authority of the Controller or Processor.

PRINCIPLES OF PERSONAL DATA PROCESSING

GXO processes personal data in accordance with the Regulation, ensuring the
following principles are upheld:

1. Lawfulness, fairness, and transparency — Personal data is processed lawfully and transparently.
2. Purpose limitation — Data is collected for specified and legitimate purposes only.
3. Data minimization — Only necessary and relevant data is processed.
4. Accuracy — Data is kept accurate and up to date.
5. Storage limitation — Data is retained only as long as necessary for its intended purpose.
6. Integrity and confidentiality — Data is processed securely to prevent unauthorized access,
loss, or damage.

WHAT PERSONAL DATA DO WE PROCESS?

To provide services in compliance with regulations, GXO processes the
following personal data:

1. Identification data — Name, surname, personal identification number, date of birth, details
from an identification document (passport or identity card).

2. Contact information — Address, phone number, email address.

3. Tax residence data — Country of birth, country of residence, taxpayer number, citizenship.

4. Communication records — Emails, letters, telephone calls (with or without audio recording), and device data.

5. Stored information — Physical and electronic documents related to the user.

6. Investment and cryptocurrency data — Cryptocurrency balance, incoming and outgoing
transfers, commissions, and other virtual currency fees.

7. Financial knowledge data — Education, knowledge, and experience in investment.

8. Transaction history — Services used, requests, complaints, and agreement performance.

9. Financial data — Sources of funds, accounts, financial liabilities, expenses, and income.

10. Economic activity data — Employment, business activity, income stability, and business
partners.

LEGAL BASES FOR PROCESSING PERSONAL DATA

We process your personal data on at least one of the following legal grounds:

• Performance of a contract — To provide services you request.

• Legal obligations — To comply with regulatory requirements, including anti-money laundering laws.

• Consent — When you explicitly agree to data processing for a specific purpose.

• Legitimate interest — To ensure service efficiency and legal compliance.

PURPOSES OF PERSONAL DATA PROCESSING

We process your personal data for the following main purposes:

1. Service provision — To establish, manage, and fulfill contractual agreements.

2. Risk assessment — Evaluating risks related to transactions and clients.

3. Cryptographic asset protection — Ensuring the security of client assets.

4. Compliance and regulatory reporting — Meeting legal and administrative requirements.

Additional purposes include:

- Identifying users.
- Ensuring contract fulfillment and service improvement.
- Evaluating financial knowledge and advising on digital payments.
- Managing customer relationships and complaints.
- Marketing activities (with consent).
- Compliance with anti-money laundering (AML) regulations.
- Reporting to public and law enforcement authorities.

HOW DO WE COLLECT PERSONAL DATA?

We collect personal data:

1. Directly from you:
   - When applying for services.
   - Through communication via post, email, phone, or in-person contact.
2. Automatically when using our services:
   - Website visits and usage data.
3. From third parties:
   - Business partners conducting market research.
   - Publicly available databases and regulatory authorities.
   - Law enforcement agencies, as required by law.

RECIPIENTS OF PERSONAL DATA

We may share personal data with:

1. Service intermediaries and transaction-related third parties.
2. Regulatory and supervisory authorities, such as tax offices and law enforcement.
3. Competent state institutions, courts, or enforcement agencies when legally required.
4. Database providers and registries that are legally established.

Access to your personal data is strictly limited to authorized employees and partners, who

process data in compliance with this policy and legal requirements.

AUTOMATED DECISION-MAKING AND PROFILING

We may use automated decision-making and profiling in:

- Marketing — To tailor relevant offers based on your preferences.
- Risk assessment — To analyze financial risks and detect unusual transactions.
- Service recommendations — To assess the suitability of financial products.

You have the right to object to automated decision-making that has significant effects on you.

DATA STORAGE AND RETENTION

Personal data is stored within the European Union (EU) and European Economic Area (EEA).

The retention period depends on:

1. Service agreements — Data is stored while the contract is active.
2. Legal obligations — AML laws require data retention for 5 years.
3. Litigation protection — Some data may be kept for up to 10 years after service termination.
4. Legitimate interests — Data may be stored longer if required for evidence or compliance.