

Privacy Statement

Last updated: 2 February 2026

Your privacy matters to us. This statement explains how Norinchukin Bank Europe N.V. (NBE) processes personal data in accordance with the EU General Data Protection Regulation (GDPR), the Dutch Data Protection Act (UAVG/AVG), and guidance issued by the Autoriteit Persoonsgegevens (AP). We are committed to handling personal data lawfully, fairly, and transparently.

1. Who This Applies To

This Privacy Statement applies to:

- individuals connected to NBE's corporate customers (.e.g., legal representatives, authorized signatories, ultimate beneficial owners, directors, shareholders, guarantors, and other persons involved in transactions or services provided by NBE).
- Visitors to our office.
- Individuals who communicate with us via email, phone, or other communication channels.
- Supplier, outsourcing partners, and vendor contacts.
- Individuals visiting our website.

NBE does not provide retail banking services.

2. What is Personal Data?

"Personal data" means any information relating to an identified or identifiable natural person.

3. Who Controls Your Data

The data controller responsible for the processing of your personal data is:

Norinchukin Bank Europe N.V.

Address: Gustav Mahlerlaan 1216, 4th Floor, 1081 LA Amsterdam, the Netherlands

Chamber of Commerce (KvK): 72676094

Telephone: +31 (0) 20 246 0700

Where relevant, other group entities may act as data processors. These are:

Norinchukin Bank (Japan)

Norinchukin, London Branch (UK)

For more detailed information about how we process personal data, including our governance framework and compliance measures, please refer to our Privacy Policy, available upon request.

4. Contact us

If you have questions about how your personal data is processed, or if you wish to exercise your rights under the GDPR, you may contact us at lc_group@nochubank.eu

5. What Personal Data We Collect

We process personal data required to meet legal and regulatory obligations, including anti-money laundering (AML), counter-terrorism financing (CFT), tax compliance, fraud prevention, and sanctions screening and other financial regulations. This includes:

1. Identification and Verification / KYC data
 - Name, date and place of birth
 - Address and country of residence
 - Government-issued ID details (including dates of issue/expiration)
 - Nationality
 - Specimen signature
 - Fiscal code
 - Any identifiers used in internal systems for compliance checks

The personal data referenced above is processed in relation to all relevant parties within the customer structure, including ultimate beneficial owners (UBOs), principals, directors, legal representatives, and shareholders.

2. Sensitive Data (AML/CFT Context)
 - Criminal conviction data (only where legally permitted and proportionate)
 - Special categories of data for sanctions screening or risk assessment
3. Audio-Visual Data (Used for fraud prevention, market abuse detection, and responding to competent authorities)
 - Surveillance recordings at premises
 - Recordings of calls, video conferences, and online chats

In addition, we process for operational, contractual, and relationship management purposes:

1. Contact and Communication Details
 - Email address, business address, telephone number
 - Job title
2. Professional Details
 - Signing authority
 - Company mandate
3. Socio-Demographic Data (Business Context)
 - Education and employment details of shareholders, directors, or senior officers
4. Supplier Contact Data
 - Identification and professional details for managing contractual relationships and legal obligations

6. How We Collect Your Personal Data

We collect data:

- Directly from you (forms, emails, calls, meetings).
- Indirectly from your employer (e.g., KYC documentation, onboarding files).
- From public sources (company registers, sanction lists, PEP lists).

- From financial institutions involved in transactions.
- From regulators and supervisory authorities.
- From trusted service providers (KYC/AML screening providers, IT service providers).

Website: NBE does not use cookies or tracking technologies on its website. No personal data is collected via the NBE website.

7. Why We Process Your Data

We process personal data on the following legal bases:

- To comply with legal and regulatory obligations, including anti-money laundering laws, FATCA, CRS, and other banking regulations.
- To perform contractual obligations with our customers.
- For our legitimate interests, such as managing business relationships and improving internal processes. In such cases, we conduct a balancing test to ensure these interests do not override your rights and freedoms.
- With your consent, where required.

8. Purposes of Processing

We use your personal data to:

- Provide and administer financial products and services.
- Perform due diligence, identity verification and integrity checks.
- Comply with statutory reporting obligations and regulatory requirements.
- Prevent fraud and financial crime.
- Manage risk, internal audits, and dispute resolution.
- Maintain secure systems and protect the integrity of the financial system.
- Respond to inquiries from competent authorities and meet international tax compliance obligations (FATCA, CRS).

9. Sharing of Personal Data

We share personal data only when necessary and in accordance with legal requirements. Recipients may include:

- Regulators and supervisory authorities such as the European Central Bank and De Nederlandsche Bank.
- Other financial institutions involved in transactions.
- Service providers supporting our operations, such as IT and cloud services.
- Norinchukin Group entities.
- Auditors, legal advisors, and other professional service providers.
- SWIFT, as a joint controller for payment processing.

Third-party processing is governed by data processing agreements and technical/organizational safeguards.

10. Transfers Outside the EEA

Where personal data is transferred outside the European Economic Area, we ensure appropriate safeguards such as Standard Contractual Clauses or Binding Corporate Rules approved by regulators. Transfers may also rely on adequacy decisions by the European Commission, where applicable. These measures guarantee that your data remains protected in line with GDPR.

You may request a copy of the transfer safeguards via the contact details above.

11. Data Retention

We retain personal data only as long as necessary for the purposes listed above, or as required by law. For example:

- Wwft (AML/KYC): 5 years after end of business relationship.
- Contract & financial records: 7 years under Dutch tax law (AWR).
- Claims/loan administration: up to 10 years (Dutch limitation period).
- General business correspondence: up to 7 years.

All retention periods are applied consistently with our internal retention schedule.

12. Your Rights

You have the right to access, rectify, erase, restrict or object to the processing of your personal data, and to data portability, where applicable. Where processing is based on consent, you have the right to withdraw consent at any time without affecting the lawfulness of processing before withdrawal. You also have the right to lodge a complaint with the Autoriteit Persoonsgegevens. We encourage you to contact us first so we can address your concerns before you approach the supervisory authority. These rights may be subject to limitations under applicable law.

Identity verification forms part of the rights process, consistent with our internal procedures (e.g., identity checks documented in the access, rectification, and erasure workflows). Requests will be processed within one month, extendable in complex cases, as required by Articles 12 and 15 GDPR.

In accordance with Article 82 of the General Data Protection Regulation (GDPR), you have the right to seek compensation for any material or non-material damage suffered as a result of a breach of data protection law. This right can be exercised through the competent courts.

You can exercise your rights or reach out to us for any questions using the contact details in par. 4.

13. Data Breaches

If a breach poses a high risk to your rights and freedoms, we will notify you promptly, as required by GDPR Article 34.

14. Automated Decision-Making

We do not carry out automated individual decision-making that produces legal or similarly significant effects. Any decisions with impact are made by humans.

15. Direct Marketing

We do not use your personal data for direct marketing purposes.

16. Security of Your Personal Data

We apply appropriate technical and organisational measures, including encryption, access controls, and monitoring, to protect your personal data.

17. Updates to This Privacy Statement

NBE maintains internal policies, procedures, and controls to ensure compliance with GDPR and AVG, including measures for data minimisation, retention, security, and rights management. These are reviewed regularly as part of our governance framework.

We may update this Privacy Statement when necessary to reflect changes in our processing activities, legal requirements, or guidance from the Autoriteit Persoonsgegevens or EDPB.

The latest version will always be available on our website.