OBNA Bank N.V.

Data Privacy Policy

Version: 1.0

Classification: Public

Effective Date: March 1st, 2026

Owner: Data Protection Officer

Approved by: Board of Directors

Your Privacy at OBNA Bank – A Simple Language Summary

This section explains our privacy practices in plain, everyday language. The full legal text follows below. Both sections form part of this policy.

At OBNA Bank, protecting your personal information is a core part of how we do business. We only collect the information we need to serve you, meet our legal obligations, and keep your money and data safe. We never sell your personal information to anyone.

Here is a quick overview of what we collect and why:

What we collect	Why we collect it
Name, address & ID documents	To open and manage your account and comply with the law
Transaction & account activity	To provide banking services and detect fraud
Device & online banking data	To secure our systems and improve your experience
Contact details	To communicate with you about your account
Credit & income information	To assess credit applications

Your key rights include accessing your data, correcting mistakes, requesting deletion, and objecting to certain uses. Where technically feasible, the Bank may provide your data in a structured electronic format upon request. These rights are explained in detail in Section 7 below.

We use cookies on our website and online banking platform. You will always be asked for your consent before any non-essential cookies are placed on your device. See Section 10 for details.

If you ever have questions or concerns, our Data Protection Officer is available to help. Contact details are in Section 17.

1. Introduction

OBNA Bank N.V. (“the Bank”) is committed to protecting the privacy and confidentiality of the personal data entrusted to us by our customers, employees, business partners, and other stakeholders. As a financial institution licensed and supervised by the Central Bank of Curaçao and Sint Maarten (CBCS), the Bank processes personal data in accordance with the Landsverordening Bescherming Persoonsgegevens (LBP), the privacy law of Curaçao.

The Bank additionally aligns its practices with recognised international data protection standards and frameworks, including the General Data Protection Regulation (GDPR), recognising that Curaçao is actively modernising its data protection framework and that many of our customers, partners, and correspondent banking relationships extend into jurisdictions governed by these instruments.

This policy sets out the principles, responsibilities, and practices that govern how the Bank collects, processes, retains, shares, and secures personal data. It reflects our commitment not only to legal compliance but to earning and maintaining the trust of everyone whose data we hold.

2. Purpose and Scope

This policy aims to safeguard the rights and freedoms of individuals whose personal data is processed by the Bank, to ensure compliance with the Laws and regulations and other applicable legal requirements, to meet supervisory expectations of the CBCS, and where relevant and consistent with the applicable law, to take into account recognised international privacy standards. It also seeks to provide clarity and transparency to customers, employees, and business partners regarding how their data is used.

This policy applies to all employees, contractors, temporary staff, and third parties acting on behalf of the Bank. It covers all personal data processed in the context of the Bank’s operations, including retail banking, lending, credit assessments, mobile and online banking, website operations, marketing activities, human resources and employment activities, and outsourcing arrangements.

3. Legal Basis for Processing

The Bank processes personal data only where a valid legal basis exists under the LBP and other applicable laws and regulations. The legal bases on which we rely include the following:

Performance of a contract: where processing is necessary to enter into or perform a contract with you, such as opening a bank account, executing a payment instruction, or processing a loan application.

Compliance with a legal obligation: where processing is required by law, including obligations under anti-money laundering and counter-terrorism financing legislation, tax reporting requirements, and supervisory reporting to the CBCS.

Legitimate interests: Processing necessary for the legitimate interests pursued by the Bank, provided that such interests are not overridden by the rights and freedoms of the data subject, in accordance with the Landsverordening Bescherming Persoonsgegevens. Examples include fraud prevention, network and information security, and the management of credit risk.

Consent: where processing requires your explicit agreement, primarily in the context of direct marketing communications, certain profiling activities, and the placement of non-essential cookies. You have the right to withdraw consent at any time without penalty, as described in Section 7.

4. Data Privacy Principles

The Bank adheres to the following principles in all its data processing activities. These principles are not merely procedural requirements; they reflect the values that underpin our approach to privacy.

Lawfulness, fairness, and transparency: we process personal data only on a lawful basis, in a manner that is fair to individuals, and with appropriate transparency regarding the purpose and methods of processing.

Purpose limitation: personal data is collected for specified, explicit, and legitimate banking purposes and is not processed in any manner that is incompatible with those purposes.

Data minimisation: we collect and retain only the data that is necessary and proportionate to the purpose for which it is processed.

Accuracy: we take appropriate measures to ensure that personal data is accurate and, where necessary, kept up to date. Customers may request corrections through the process described in Section 7.

Storage limitation: personal data is retained only for as long as is necessary to fulfil its processing purpose or as required by law, in accordance with the retention schedule in Section 13.

Integrity and confidentiality: we process personal data securely, using appropriate technical and organisational measures to prevent unauthorised access, loss, destruction, or damage.

Accountability: the Bank accepts responsibility for compliance with these principles and maintains records and procedures that enable us to demonstrate that compliance.

5. Roles and Responsibilities

Board of Directors: the Board holds ultimate accountability for ensuring the Bank's compliance with its data privacy obligations and approves this policy annually.

Data Protection Officer (DPO): the Bank has appointed a DPO in accordance with the requirements of the LBP and other applicable legal requirements. The DPO is responsible for advising the Bank on compliance matters, monitoring adherence to this policy, handling data subject requests and

complaints, and serving as the point of contact with the supervisory authority. The DPO operates with the professional independence required by applicable law and reports directly to the Board of Directors on privacy matters. The DPO may be contacted directly using the details in Section 17.

Chief Information Security Officer (CISO): the CISO ensures that appropriate technical safeguards are in place, including encryption standards, access controls, monitoring systems, and incident response procedures.

Employees and contractors: all individuals working for or on behalf of the Bank are required to handle personal data responsibly and in accordance with this Policy. They must complete the mandatory training described in Section 14, and to report any suspected privacy incidents without delay.

Third-party vendors and processors: any third party that processes personal data on behalf of the Bank is required to do so under a written data processing agreement that includes obligations equivalent to those in this policy. Third-party processors are subject to ongoing oversight, including the right to periodic audits where appropriate.

6. Categories of Personal Data Processed

The Bank processes the following categories of personal data in the ordinary course of its operations.

Customer data: identification documents required for Know Your Customer (KYC) purposes, financial account and transaction information, credit and income data, contact details, and records of communications with the Bank.

Employee data: Human Resources (HR) and payroll records, performance assessments, attendance data, benefits information, and compliance-related records such as conduct history and professional qualifications.

Third-party and vendor data: contact details and contractual information relating to business partners, service providers, and their personnel.

Online and digital interaction data: IP addresses, device identifiers, browser type, session data, and information collected through cookies and similar technologies when you visit our website or use our online banking platform. This category is described in detail in Section 10.

Sensitive personal data: categories such as data relating to, biometric identifiers, or PEP-related records will only be processed where strictly necessary and under appropriate safeguards, including additional legal justification beyond the standard bases set out in Section 3.

7. Your Rights as a Data Subject

Under the LBP, you have the following rights in relation to your personal data. These rights are not absolute and are subject to statutory limitations, but the Bank will always assess requests fairly and provide a reasoned response.

Your right	What it means
Access	Request a copy of the personal data we hold about you.
Rectification	Ask us to correct any information that is inaccurate or incomplete.
Erasure	Request deletion of your data where it is no longer needed for a lawful purpose.
Restriction	Ask us to pause processing of your data in certain circumstances.
Objection	Object to processing based on legitimate interests or for direct marketing.
Data format request	While Curaçao law does not provide a formal right to data portability, the Bank may, where technically feasible, provide personal data in a structured electronic format upon request.
Withdraw consent	Withdraw any consent you have previously given, at any time, without penalty.
Lodge a complaint	File a complaint with the competent supervisory authority or seek recourse through the Gerecht in eerste aanleg van Curaçao, forming part of the Joint Court of Justice, if you believe your rights have been violated.

To exercise any of these rights, please submit a written request to our Data Protection Officer using the contact details in Section 17. We will acknowledge your request within five (5) business days and respond substantively within thirty (30) days, unless the complexity or volume of requests makes this impracticable, in which case we will notify you of the extended timeline.

The Bank may request proof of identity before actioning a request, to ensure that personal data is not disclosed to an unauthorised person. This is a security measure intended to protect you.

The Bank processes data subject requests free of charge. Where a request is manifestly unfounded or excessive - for example, because of its repetitive character - the Bank may charge a reasonable administrative fee that reflects the actual cost of providing the information or taking the requested action, or may decline to act on the request. In either case, the Bank will explain the reasons for its position.

Where your request is refused in whole or in part, you will receive a written explanation of the reasons and information on your right to escalate the matter to the supervisory authority or to the Gerecht in eerste aanleg van Curaçao.

Right to Withdraw Consent

Where the Bank processes your personal data on the basis of your consent - for example, for direct marketing or for non-essential cookies - you may withdraw your consent at any time by contacting us or by using the opt-out mechanism provided in the relevant communication or on our website. Withdrawal of consent does not affect the lawfulness of processing that took place before the withdrawal.

8. International Data Transfers

Personal data may be transferred outside of Curaçao in limited circumstances, for example to correspondent banks and international payment networks, IT service providers and cloud platform operators, group entities, and regulatory bodies with an international mandate. Transfers are most commonly directed to the Netherlands, the United States, and Canada, and other jurisdictions within the European Economic Area, though the Bank may use service providers in other countries where appropriate safeguards are in place.

The Bank ensures that any such transfer is subject to appropriate safeguards. The Bank ensures that any international transfer of personal data takes place with appropriate safeguards to protect the confidentiality and security of the data. Where personal data is transferred to organisations located outside Curaçao, the Bank ensures that adequate contractual, organisational, and technical measures are in place to ensure that the data remains protected in accordance with the principles of the Landsverordening Bescherming Persoonsgegevens.

These safeguards may include contractual obligations imposed on service providers, security and confidentiality requirements, and oversight mechanisms designed to ensure that personal data continues to be handled responsibly.

We give preference to service providers operating in jurisdictions recognised as adequate under internationally accepted data protection equivalence frameworks.

Where transfers are required by applicable CBCS outsourcing requirements, the Bank will additionally comply with the notification and approval procedures mandated by the Central Bank and will ensure that data protection obligations are incorporated into any outsourcing arrangement.

9. Security of Processing

The Bank maintains a comprehensive information security framework aligned to ISO 27001 and CIS Controls v8.1. Our security programme is designed to protect the confidentiality, integrity, and

availability of all personal data we hold. Business continuity and disaster recovery arrangements are maintained in line with ISO 22301.

The technical and organisational security measures we employ include role-based access controls and the principle of least privilege, ensuring that employees can only access data necessary for their specific responsibilities; multi-factor authentication for all critical and internet-facing systems; encryption of personal data both in transit and at rest using current industry-standard protocols; continuous logging, monitoring, and automated incident detection; secure backup systems with regular recovery testing; and periodic penetration testing and vulnerability assessments conducted by qualified specialists.

These measures are reviewed at least annually and are updated in response to emerging threats, changes in technology, and the findings of security assessments.

10. Cookies and Online Tracking Technologies

When you visit the Bank's website or use our online banking platform, we may use cookies and similar technologies to support the functionality, security, and performance of our digital services. This section explains what these technologies are, how we use them, and how you can control them.

A cookie is a small text file stored on your device by your web browser. Some cookies are essential for the website to function correctly; others are optional and serve additional purposes such as analytics or personalisation. We use the following categories of cookies.

Essential Cookies

These cookies are strictly necessary for the website and online banking platform to operate. They enable functions such as logging in securely, navigating between pages, and completing transactions. Because they are necessary for the operation and security of the website and online banking platform, these cookies may be used without requiring prior consent. You may disable them through your browser settings, but doing so will prevent you from using core banking functions.

Functional Cookies

These cookies allow the website to remember choices you have made - such as your preferred language or whether you have agreed to certain terms - and to provide enhanced features. They are optional and will only be placed with your consent.

Analytics and Performance Cookies

These cookies collect information about how visitors use our website, such as which pages are visited most frequently and whether error messages are received. This information is used in aggregate and anonymised form to improve the website's performance. These cookies will only be placed with your consent.

Third-Party Cookies

Some pages on our website may include content provided by third parties, such as embedded maps or social media sharing buttons. These third parties may set their own cookies. The Bank does not control third-party cookies and encourages you to review the privacy policies of those third parties directly.

When you first visit our website, you will be presented with a cookie consent banner that allows you to accept or decline each category of optional cookie. You may change your preferences at any time by accessing the cookie settings link in the website footer. Withdrawing consent for optional cookies does not affect the lawfulness of any processing that took place while your consent was in effect.

The Bank does not use cookies or tracking technologies to build individual profiles for sale to advertisers or third-party data brokers.

11. Automated Decision-Making and Profiling

As a bank, we use automated systems to assist in decision-making across a range of activities, including credit scoring for loan and overdraft applications, transaction monitoring for fraud and money laundering detection, and risk-based assessments for Know Your Customer (KYC) screening. These processes are a normal and necessary part of modern banking operations and are used to protect customers as well as to fulfil our regulatory obligations.

Where the Bank uses automated systems to support decision-making, such systems are designed to assist human decision-makers and to improve consistency and efficiency.

The Bank ensures that individuals are not subject to decisions that produce significant legal or comparable effects and that are based solely on automated processing, unless such processing is permitted by law or necessary for entering into or performing a contract with the individual, and appropriate safeguards are in place.

Where an individual believes that an automated assessment has resulted in an incorrect outcome, they may contact the Bank to request that the decision be reviewed.

You also have the right to ask us to explain the principal factors that influenced the automated outcome, and to contest a decision you believe to be incorrect. To exercise these rights, please contact our DPO using the details in Section 17.

Our automated profiling systems do not use sensitive characteristics such as race, religion, health status, or political opinion as input factors. The Bank reviews its automated decision models periodically to identify and mitigate bias, and to ensure that outcomes remain fair and consistent with legal requirements.

Privacy Risk Assessments

Before introducing or materially modifying processing activities that may pose elevated privacy risks, the Bank performs a structured privacy risk assessment. These assessments—often referred to internationally as Data Protection Impact Assessments (DPIAs)—evaluate the necessity, proportionality, and potential risks of the proposed processing and identify measures to mitigate those risks. The assessments are reviewed by the Data Protection Officer and form part of the Bank's internal privacy governance framework. These assessments support the Bank's obligation to ensure that personal data is processed in a careful and proportionate manner under the Landsverordening Bescherming Persoonsgegevens.

12. Data Breach Management

All employees are required to report a suspected or confirmed data breach immediately upon discovery to the DPO and CISO. The Bank has established a documented incident response procedure that ensures prompt action to contain any breach, assess its scope and likely impact, and initiate the appropriate notifications.

Where a breach is likely to result in a significant risk to the rights and freedoms of affected individuals, the Bank will notify the relevant supervisory authority without undue delay after becoming aware of the breach, in line with recognised international best practice. Where the breach is likely to result in a high risk to specific individuals, those individuals will also be notified without undue delay, in a clear and plain-language communication that explains what occurred, what data was affected, and what steps they can take to protect themselves.

All incidents - including those assessed as low risk - are recorded in a breach register maintained by the DPO. This register is reviewed periodically to identify patterns and to improve the Bank's preventive controls.

13. Retention and Disposal

Personal data is retained only for as long as is necessary to fulfil the purpose for which it was collected, or as required by applicable law and CBCS supervisory guidance. The following retention periods apply as a baseline, subject to any specific legal requirement that mandates a longer or shorter period.

Customer account data (including KYC documentation, account opening records, and related correspondence): retained for ten (10) years following account closure, in accordance with CBCS regulatory requirements and Curaçao civil limitation periods.

Transaction records: retained for a minimum of ten (10) years from the date of the transaction, consistent with tax reporting and audit requirements.

AML/CFT records (including transaction monitoring outputs and suspicious activity reports): retained for a minimum of five (5) years from the date of the underlying transaction or the end of the business relationship, extendable to seven (7) years where required by competent authority or in the context of

ongoing investigations or legal proceedings. Retention may be extended further where required by judicial order, regulatory directive, or ongoing law enforcement proceedings.

Employee records (including HR files, payroll records, and performance documentation): retained for seven (7) years following the end of the employment relationship, to satisfy obligations under labour law and tax legislation.

Website and online banking interaction logs (including session data and cookie-related data): retained for thirteen (13) months from the date of collection unless a shorter period is technically required or the individual has withdrawn consent for the relevant processing.

At the end of each applicable retention period, personal data will be securely and irreversibly destroyed. Destruction methods include certified data wiping for electronic records, cryptographic erasure for cloud-hosted data, and cross-cut shredding for physical documents. Destruction is documented and records of disposal are maintained by the CISO.

14. Training and Awareness

The Bank recognises that data privacy is not solely a technical or legal matter; it depends on the daily decisions and behaviours of every person who works with personal data. Accordingly, mandatory privacy and information security training is provided to all employees at the time of joining and refreshed on an annual basis thereafter.

Employees in roles with elevated data access or privacy risk - including those in IT, compliance, customer-facing operations, and credit underwriting - receive additional role-specific training covering their particular responsibilities and the controls relevant to their work. Awareness campaigns are conducted throughout the year to reinforce secure data handling practices and to communicate updates to policy, law, or the threat environment.

Completion of mandatory training is tracked by the DPO and reported to the Board of Directors as part of the annual privacy compliance review.

15. Monitoring and Audit

Compliance with this policy is subject to ongoing monitoring through a combination of internal audit activity, technical system controls, and periodic external review. The Bank periodically conducts a formal internal privacy review, covering the adequacy of data processing activities, the effectiveness of privacy controls, and the currency of data subject rights procedures.

External specialists are engaged as needed to provide independent assurance, including penetration testing of systems that process personal data, and periodic reviews of the Bank’s compliance with ISO

27001 and the LBP. Findings from both internal and external reviews are reported to the Board of Directors and tracked to resolution through a formal remediation process.

16. Governance and Review

This policy is reviewed at least annually by the DPO and submitted to the Board of Directors for approval. Reviews are brought forward where significant changes in applicable laws, supervisory guidance, or the Bank's business operations make an update necessary. The version history of this policy - including the date of each revision and the nature of the changes made - is maintained in the Bank's policy register and is available upon request.

Employees and stakeholders will be informed of any material changes to this policy through appropriate communication channels.

17. Contact and Complaints

If you have any questions about this policy, wish to exercise any of your data subject rights, or have a concern about how your personal data has been handled, please contact the Bank's Data Protection Officer in the first instance. We are committed to addressing your concerns promptly and fairly.

Data Protection Officer
OBNA Bank N.V.
Schotteweg Ost 3C
Email: dpo@obna-bank.com]
Telephone: +599 9 843 3000

If you are not satisfied with the Bank's response, you may seek recourse through the competent authority responsible for the protection of personal data in Curaçao, or through the Gerecht in eerste aanleg van Curaçao forming part of the Gemeenschappelijk Hof van Justitie van Aruba, Curaçao, Sint Maarten en van Bonaire, Sint Eustatius en Saba (Joint Court of Justice).

As Curaçao continues to develop its data protection institutional framework, the Bank will update this section to reflect any changes in the designated supervisory authority for privacy matters.

As a licensed financial institution, the Bank is supervised by the Central Bank of Curaçao and Sint Maarten (CBCS) with respect to prudential and operational matters. Privacy-related concerns may therefore also be raised with the Bank directly or through the relevant judicial channels.

18. Governing Law

This policy and any matters arising from or connected with it are governed by and construed in accordance with the laws of Curaçao. Any dispute arising from the application or interpretation of this policy that cannot be resolved by the Bank's internal complaints procedure may be submitted to the the Gerecht in eerste aanleg van Curaçao, forming part of the Gemeenschappelijk Hof van Justitie (Joint Court of Justice), in accordance with applicable procedural law.