

SONNE N.V.

Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy

Version 2.0

Table of Contents

<i>Key Information.....</i>	<i>3</i>
<i>1. Policy Statement.....</i>	<i>4</i>
<i>2. Purpose.....</i>	<i>5</i>
<i>3. Audience.....</i>	<i>6</i>
<i>4. Definitions.....</i>	<i>7</i>
<i>5. Policy Implementation.....</i>	<i>8</i>
<i>5.1. Information Entered on Registration.....</i>	<i>8</i>
<i>5.2. Terms Acceptance.....</i>	<i>8</i>
<i>5.3. Underage Customers.....</i>	<i>8</i>
<i>5.4. Business Risk Assessment (BRA).....</i>	<i>8</i>
<i>5.5. Customer Risk Assessment (CRA).....</i>	<i>9</i>
<i>5.6. Customer Acceptance Policy (CAP).....</i>	<i>11</i>
<i>5.7. Customer Due Diligence (CDD).....</i>	<i>12</i>
<i>▪ CDD Measures:.....</i>	<i>12</i>
<i>▪ Enhanced Due Diligence (EDD):.....</i>	<i>13</i>
<i>▪ Procedure for B2B Clients (KYB):.....</i>	<i>13</i>
<i>5.8. Ongoing Monitoring.....</i>	<i>13</i>
<i>5.9. Reliance on Third Parties for CDD.....</i>	<i>14</i>
<i>5.10. Reporting of Suspicious Transactions.....</i>	<i>14</i>
<i>5.11. Anti-Money Laundering Compliance Program.....</i>	<i>15</i>
<i>6. Compliance and Consequences of Non-Compliance.....</i>	<i>17</i>
<i>7. Related Information.....</i>	<i>18</i>
<i>8. Contact Information.....</i>	<i>19</i>
<i>9. Policy History.....</i>	<i>20</i>
<i>10. Policy URL.....</i>	<i>21</i>
<i>Appendix 1.....</i>	<i>22</i>

Key Information

Approving Official(s):

- Morganite Corporate Services B.V, Director SONNE N.V.

Responsible Office:

- Compliance Department, SONNE N.V.

Effective Date:

- March 19, 2025

Next Review Date:

- March 19, 2026 (initial review within one year, subsequent reviews every three years)

1. Policy Statement

SONNE N.V. ("the Company"), a Curaçao-incorporated (Registration No. 163610; Registration address: Abraham de Veerstraat 1, Curacao; has a valid license issued by the Curaçao Gaming Authority), is committed to preventing its services, products, and facilities from being used for money laundering (ML), terrorist financing (TF), or the financing of proliferation of weapons of mass destruction (FP). The Company adheres to Curaçao laws, including the National Ordinance on Identification when Rendering Services (NOIS, N.G. 2017, no. 92), the National Ordinance on the Reporting of Unusual Transactions (NORUT, N.G. 2017, no. 99), the National Ordinance on Games of Chance (NOGC, N.G. 2024, no. 124), the National Ordinance Penalization of Money Laundering (NOPML), the Sanctions National Ordinance (N.G. 2014, no. 55), and the Kingdom Sanction Act (N.G. 2016, no. 54). Additionally, the Company aligns with the FATF Recommendations and EU Directives 2015/849, 2018/843, and 2018/1673. This policy applies to all employees, contractors, third-party agents, and business partners involved in the Company's operations.

2. Purpose

This AML/CTF Policy ensures compliance with Curaçao's legal framework and international standards, including the "Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction" (effective January 9, 2025), FATF Recommendations, and EU Directives. The policy aims to:

- Protect the Company's reputation and operations from financial crime risks.
- Implement a risk-based approach to identify, assess, and mitigate ML/TF/FP risks.
- Ensure robust customer due diligence (CDD), know-your-business (KYB), transaction monitoring, and reporting of suspicious activities.
- Establish procedures for screening and monitoring B2B clients to comply with the Company's requirements.
- Foster a culture of compliance through employee training, background checks, and internal controls.
- Prevent predicate offenses to ML/TF, such as fraud, as defined in EU Directive 2018/1673 and other legislative acts.

3. Audience

This policy applies to:

- All employees, officers, and directors of SONNE N.V.
- Third-party service providers, agents, and subcontractors involved in the Company's operations.
- B2C customers (players) and B2B clients (business partners, such as platform providers or operators using the Company's services or Company's platform).

4. Definitions

- **Casino:** Refers to SONNE N.V. online gaming operations.
- **Financial Transactions:** Deposits, withdrawals, wire transfers, and currency exchanges (excluding gambling transactions like wagers or winnings).
- **FIU:** Financial Intelligence Unit Curaçao, responsible for receiving suspicious activity reports (SARs).
- **Politically Exposed Persons (PEPs):** Individuals entrusted with prominent public functions, their family members, or close associates, as defined in EU Directive 2015/849 and other legislative acts.
- **Suspicious Transaction:** A transaction meeting objective or subjective indicators under NORUT, such as transactions $\geq$ NAf. 5,000 or suspected ML/TF activity.
- **Ultimate Beneficial Owner (UBO):** Natural person(s) who own or control a customer or entity, holding $\geq 25\%$ shares/voting rights or exercising ultimate control, per EU Directive 2018/843 and other legislative acts.
- **Source of Funds (SoF):** Origin of funds for a specific transaction (e.g., salary, gambling winnings).
- **Source of Wealth (SoW):** Origin of a customer's accumulated wealth (e.g., employment, investments).
- **Predicate Offense:** Criminal activities generating proceeds that may be laundered, as outlined in EU Directive 2018/1673 (e.g., fraud, corruption).

5. Policy Implementation

The Company adopts a risk-based approach to AML/CTF compliance, as mandated by the Curaçao Gaming Authority (CGA, formerly Curaçao Gaming Control Board) and FATF Recommendations. The following sections outline the implementation framework.

5.1. Information Entered on Registration

During the registration process and later on, the Company will request the following identifying information and contact details:

- First Name and Last Name.
- Date of Birth.
- Passport document details ID-card/driver's license.
- Gender.
- Country of Residence.
- Address.
- Email address and mobile number.
- Username and Password.

5.2. Terms Acceptance

During the registration process, the customer must also confirm acceptance of the website's.

5.3. Underage Customers

The system does not allow registration of customers who are underage: In order for the registration process to be successful, customers must be at least 18 years old or of legal age in their territory. Date of Birth will be cross checked with the provided ID upon customer Due Diligence.

5.4. Business Risk Assessment (BRA)

Objective: Identify and mitigate ML/TF/FP risks inherent to the Company's operations.

Procedure:

- The Compliance Department conducts an annual BRA, updated upon significant changes (e.g., new products, markets, or regulations).
- The BRA evaluates:
 - **Customer Risk:** Risks from high spenders, PEPs, or customers with irregular income.
 - **Geographical Risk:** Exposure to high-risk jurisdictions (e.g., FATF High-Risk

Jurisdictions <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>, EU Directive 2018/843 Annex II countries).

- **Product/Service Risk:** Risks from products allowing anonymity (e.g., prepaid cards, cryptocurrencies) or high-stake games (e.g., roulette).
- **Distribution Channel Risk:** Risks from non-face-to-face interactions or third-party intermediaries.
- Sources consulted include FATF lists, CFATF statements, Transparency International's Corruption Perceptions Index, EU sanctions lists, and the U.S. INCSR.
- The BRA is documented, approved by the Board of Directors, and submitted to the CGA upon request.
- Outcomes inform the Company's risk appetite and AML/CTF controls, ensuring alignment with FATF Recommendation 1 (risk-based approach).

5.5. Customer Risk Assessment (CRA)

Objective: Assess ML/TF/FP risks posed by B2C players and B2B clients.

Procedure for B2C Customers:

- Conducted at onboarding and updated during the business relationship.
- Factors assessed (per FATF Recommendation 10 and EU Directive 2015/849):
 - **Individual Status:** PEP status, sanctions/blacklist presence, adverse media.
 - **Geographical Location:** Residence in high-risk countries (e.g., FATF black/grey lists, Appendix 1).
 - **Gambling/Transactional Behavior:** Large deposits with minimal play, smurfing, or disproportionate spending.
 - **Payment Methods:** Use of high-risk methods (e.g., vouchers, cryptocurrencies, prepaid cards). Payment Methods are also divided into:

Payment Method	Risk Rating
Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks	Low
EEA licensed e-wallets (Skrill, Neteller, paysafecard)	Medium
Vouchers, cryptocurrencies, prepaid cards	High

- **Fraud Indicators:** VPN usage, multi-accounting, or synthetic identities.
- Risk ratings (low, medium, high) determine CDD levels:
 - **Low (0–20):** Basic CDD, minimal monitoring.
 - **Medium (21–40):** Standard CDD, additional personal details, SoF checks.
 - **High (41+):** Enhanced Due Diligence (EDD), SoF/SoW documentation, enhanced

monitoring.

- Risk scores are calculated based on weighted indicators (e.g., PEP status: 100 points, high-risk country: 30 points). More details in the table below:

Indicator	Description	Score
individual status		
PEP	A customer considered to be PEP	100
Adverse media	A customer was mentioned in negative news or information the company discovered from various sources	50
Sanctions/blacklist	A customer is under international sanctions/blacklists	100
geographical location		
Not at home	A customer whose IP location is different from their registered address	20
High-risk countryresident	A customer resides in a High-risk country	30
gambling behavior		
Large sums no play	A customer depositing large sums, then places minimal stake bets, then withdrawing all their funds	50
Large sums biglosses	A customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence(EUR 5000 per week)	50
Low odds betting	A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favorites) bets	25
Big changes inmoney	Dramatic changes in terms of volume and size of player deposits or staking activity	20
Several gaming accounts	A customer is trying to register several gaming accounts	30
transactional behavior		
Smurfing	A customer making multiple deposits or withdrawals of small amounts without no objective reasons	30
Spending above wages	A customers spend is outside of their affordability	20
No withdrawals	Player has never requested a withdrawal	-20

Withdrawal without playing	Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling	30
payment methods the player is using		
Card switching	A customer opening an account and registering several different cards and making transfers between them	20
High risk payment methods	A customer uses high-risk payment methods	30
fraud red flags a customer triggered		
VPN	Customer used a VPN	30

Procedure for B2B Clients:

- Prior to establishing a B2B relationship, the Compliance Department assesses:
 - Client's AML/CTF policies and compliance with Curaçao regulations.
 - UBOs ($\geq 25\%$ ownership/control) and directors, per EU Directive 2018/843.
 - Geographical risks associated with the client's operations or headquarters.
 - Nature of services provided (e.g., platform-sharing, white-label solutions).
- B2B clients are screened against UN, EU, and Curaçao sanctions lists (e.g., N.G. 2015, no. 27–30, 65) and PEP databases.
- Risk ratings guide ongoing monitoring and contract terms.

5.6. Customer Acceptance Policy (CAP)

Objective: Define criteria for accepting B2C and B2B customers.

Procedure:

- The CAP specifies:
 - **High-Risk Customers:** PEPs, sanctioned entities, residents of FATF black/grey-listed countries (Appendix 1), or those with adverse media.
 - **Risk Indicators:** Multiple accounts, high-risk payment methods, or fraud red flags.
 - **CDD Measures:** Simplified (SDD), standard, or enhanced (EDD) based on risk level.
 - **Grounds for Rejection:**
 - ✓ Underage individuals (< 18).
 - ✓ Sanctioned entities or PEPs (automatic rejection per EU Directive 2015/849), the Consolidated United Nations Security Council Sanctions List 12, the Sanction Decree “Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s.” (N.G. 2015, no. 29), the Ministerial Regulation “Libya” (N.G. 2015, 28), the Sanction

Decree “Islamic Republic Iran 2015” (N.G. 2015, 27);, the Sanction Decree “Democratic People’s Republic of Korea 2015” (N.G. 2015, 30), and the Ministerial Regulation “Yemen” (N.G. 2015, 65).

- ✓ Incomplete CDD within 14 days.
- ✓ Fraudulent behavior, bonus abuse, or terms breaches.
- ✓ Existing customers who have an existing exclusion on the site.
- ✓ Individuals with fraud red flags.
- ✓ B2B clients with inadequate AML/CTF controls.
- ✓ Entities directly or indirectly owned by any PEP.
- B2C customers are declined if they fail to provide CDD documentation or are listed on sanctions lists.
- B2B clients are declined if they lack adequate AML/CTF policies or are non-compliant with Curaçao regulations.
- Geo-blocking restricts access from prohibited jurisdictions (Appendix 1).

5.7. Customer Due Diligence (CDD)

Objective: Verify customer identities and mitigate ML/TF/FP risks, per FATF Recommendation 10 and EU Directive 2015/849.

Procedure for B2C Customers:

- **When CDD is Required:**
 - Financial transactions $\geq$ Naf. 4,000 or EUR 2,000 (single or linked), per EU Directive 2018/843.
 - Suspected ML/TF activity or predicate offenses (e.g., fraud, per EU Directive 2018/1673).
 - Doubts about previously obtained identification data.
 - Account registration or wagering.
- **CDD Measures:**
 - **Identification:** Collect full name, residential address, date of birth, nationality, and identity number. For low-risk customers, limit to name, address, and date of birth.
 - **Verification:** Use unexpired government-issued photo ID (e.g., passport, driver’s license). Verify address via utility bills ($\leq$ 3 months old), lease agreements, or government correspondence. Biometric checks or geo-location data may be used.
 - **UBO Identification:** Ensure players act on their own behalf via terms and conditions. For syndicate-funded accounts, identify and verify UBOs.

- **Purpose of Relationship:** Establish expected activity levels using customer declarations or statistical data.
- **Sanctions/PEP Screening:** Screen against UN, EU, and Curaçao sanctions lists and PEP databases (e.g., knowyourcountry.com) at registration and every 6 months.
- **Enhanced Due Diligence (EDD):**
 - Applied for high-risk customers (e.g., PEPs, high spenders, or transactions $\geq$ EUR 2,000). Includes:
 - SoF/SoW verification (e.g., payslips, bank statements, sale contracts).
 - Senior management approval.
 - Enhanced monitoring for complex/unusual transactions.
 - **Simplified Due Diligence (SDD):** Applied for low-risk customers, limiting identification to basic details.
 - **Freezing of Funds:** If a customer is sanctioned or ML/TF is suspected, funds are frozen, and a SAR is filed with the FIU within 7 days. Accounts are blocked if CDD is incomplete after 14 days, with funds returned to the original source unless ML/TF is suspected.
 - **Ongoing Monitoring:**
 - Refresh ID upon document expiry or profile changes.
 - Monitor transactions for inconsistencies (e.g., large deposits, smurfing).
 - Conduct CDD every 6 months for verified customers.
- **Procedure for B2B Clients (KYB):**
 - **Identification:** Collect company name, registration number, address, and UBO details ($\geq$ 25% ownership/control).
 - **Verification:** Use commercial registries, Memorandum of Association, Registrar Excerpt, Register of Directors/Shareholders ($\leq$ 3 months old), active gaming license, or business plan. Notarized/apostilled documents may be requested.
 - **AML/CTF Compliance Check:** Review the client's AML/CTF policies and regulatory compliance.
 - **Sanctions/PEP Screening:** Screen UBOs and directors against sanctions lists and PEP databases.
 - **Contractual Obligations:** B2B contracts mandate compliance with Curaçao AML/CTF regulations and quarterly due diligence reviews.

5.8. Ongoing Monitoring

Objective: Ensure customer activity aligns with risk profiles and detect suspicious behavior.

Procedure for B2C Customers:

- **Identity Monitoring:** Refresh identification upon key events (e.g., payment method changes) or document expiry.
- **Transaction Monitoring:** Scrutinize transactions for inconsistencies (e.g., large deposits with minimal play, card switching). Investigate SoF for deviations.
- **Behavioral Monitoring:** Identify patterns indicative of ML/TF (e.g., low-odds betting, smurfing) or problem gambling.
- **Risk Profile Updates:** Reassess risk ratings if significant changes occur (e.g., new PEP status).
- **High-Risk Customers:** Conduct enhanced monitoring, including frequent SoF/SoW checks.

Procedure for B2B Clients:

- Monitor client transactions and compliance with AML/CTF obligations.
- Conduct quarterly audits of B2B clients' AML/CTF controls.
- Reassess risk profiles upon contract renewals or regulatory changes.

5.9. Reliance on Third Parties for CDD

Objective: Ensure compliance when delegating CDD tasks, per FATF Recommendation 17 and EU Directive 2015/849.

Procedure:

- The Company may rely on third parties (e.g., payment processors) for identification, verification, and purpose of relationship data, provided:
 - The third party is regulated and complies with Curaçao or equivalent AML/CTF standards.
 - An agreement ensures immediate access to CDD data.
 - The arrangement is tested periodically for effectiveness.
- The Company remains responsible for CRA, PEP screening, and ongoing monitoring.
- For B2B clients, third-party CDD is permitted only if the client's jurisdiction has equivalent AML/CTF standards.
- Outsourcing to agents requires the Company's AML/CTF policies to be applied, with regular compliance audits.

5.10. Reporting of Suspicious Transactions

Objective: Detect and report transactions indicative of ML/TF/FP, per FATF Recommendation 20 and EU Directive 2015/849.

Procedure:

- **Recognition:** Employees are trained to identify suspicious transactions, including:
 - Transactions $\geq$ NAf. 5,000 or EUR 2,000 (cash, cashless, chips, or withdrawals).
 - Transactions reported to authorities for ML/TF or predicate offenses.
 - Transactions involving sanctioned entities or PEPs.
 - Red flags (e.g., large deposits with minimal play, frequent small transactions, third-party withdrawals).
- **Internal Reporting:** Employees submit Internal Suspicious Activity Reports (SARs) to the Compliance Officer, including customer details, employee statements, and supporting documents.
- **External Reporting:** The Compliance Officer submits SARs to the FIU via the goAML portal within 7 days of detection, in English, with all relevant documentation.
- **Account Blocking:** If ML/TF is suspected, accounts may be blocked to prevent tipping off (per EU Directive 2015/849, Article 41). Funds are frozen if sanctions apply.
- **Tipping Off:** Employees are prohibited from informing customers about SARs or investigations to avoid prejudicing inquiries.
- **Record Keeping:** All transaction records, SARs, and CDD data are retained for ≥ 5 years post-relationship or transaction, per FATF Recommendation 11.

5.11. Anti-Money Laundering Compliance Program

Objective: Establish a robust framework to mitigate ML/TF/FP risks.

Procedure:

- **Internal Policies and Controls:**
 - Policies express senior management's commitment to AML/CTF compliance.
 - Procedures detail CDD, KYB, reporting, and monitoring processes.
 - Internal controls detect deviations (e.g., automated transaction monitoring).
- **Compliance Officer:**
 - A senior officer, independent from gaming operations, oversees the AML program.
 - Responsibilities include risk analysis, policy development, training, SAR submission, and FIU liaison.
 - The officer has authority to issue instructions and conduct random checks.
- **Employee Training:**
 - New employees receive AML/CTF training, including recognition of predicate offenses (EU Directive 2018/1673).
 - Frontline staff (e.g., cashiers) are trained on ML techniques, red flags, and reporting.

- Annual refresher training covers new trends and regulatory updates.
- Training records include content, attendees, dates, and test results.
- **Employee Background Checks:**
 - Pre-employment checks include ID, CV, and integrity assessments.
 - Annual screenings ensure compliance, with surprise checks for high-risk roles.
- **Independent Audit:**
 - Conducted annually by a qualified external auditor (≥ 2 years AML experience, CAMS certification).
 - Tests include policy evaluation, customer file reviews, transaction testing, and training adequacy.
 - Findings are reported to senior management with corrective action deadlines.
- **Account Blocking Procedure:**
 - Accounts are blocked if CDD is incomplete after 14 days, ML/TF is suspected, or sanctions apply.
 - Funds are returned to the original source unless ML/TF suspicions or sanctions require freezing and FIU reporting.

6. Compliance and Consequences of Non-Compliance

Compliance:

- All employees and third parties must adhere to this policy.
- The Compliance Officer monitors implementation and reports to senior management.

Consequences of Non-Compliance:

- **Employees:** Disciplinary actions, up to termination, for policy violations.
- **Third Parties/B2B Clients:** Termination of contracts for non-compliance.
- **Legal Risks:** Administrative fines or criminal sanctions under NOIS, NORUT, NOPML, or Sanctions National Ordinance.
- **Business Risks:** Reputational damage or license revocation by the CGA.

7. Related Information

- **Regulations:** NOIS (N.G. 2017, no. 92), NORUT (N.G. 2017, no. 99), NOGC (N.G. 2024, no. 124), NOPML, Sanctions National Ordinance (N.G. 2014, no. 55), Kingdom Sanction Act (N.G. 2016, no. 54).
- **International Standards:** FATF Recommendations, EU Directives 2015/849, 2018/843, 2018/1673.
- **Guidelines:** Curaçao CGA Regulations for combating ML/TF/FP (January 2025).
- **Resources:** UN Sanctions List, EU Sanctions Map, FATF Black/Grey Lists, Transparency International Corruption Perceptions Index.

8. Contact Information

For questions, contact:

- Compliance Department, SONNE N.V.
- Email: legal@sonne-it.org

9. Policy History

Version	Date	Approved By
1.0	September 14, 2023	Theoklis Andreou, Director
2.0	March 19, 2025	Morganite Corporate Services B.V., Director

10. Policy URL

Available at: <https://sonne.bet/page/aml-and-kyc-policy>

Signed This 19th day of March 2025

A handwritten signature in black ink is written over a horizontal line. To the right of the signature is a circular corporate seal. The seal contains the text "CORPORATE OF COMMERCE NO. 00000000" around the top edge and "MORGANITE CORPORATE SERVICES B.V." around the bottom edge. In the center of the seal is a logo consisting of a stylized 'M' and 'C'.

Director: Morganite Corporate Services B.V.

Norine Clifton
Managing Director

Appendix 1

Afghanistan
Aland Islands
American Samoa
Angola
Anguilla
Antarctica
Antigua and Barbuda
Barbados
Belize
Benin
Bhutan
Bonaire (including Sint Eustatius and Saba)
Bouvet Island
British Indian Ocean Territory
Burundi
Cape Verde
Central African Republic
Chad
Cocos (Keeling) Islands
Cook Islands
Comoros
Congo, Democratic Republic
Republic of Congo
Crimea
Cuba
Curacao
Djibouti
Equatorial Guinea
Eritrea
Fiji
French Guyana
French Polynesia
French Southern Territories
Gabon
Gambia
Greece

Grenada

Guadeloupe
Guam
Guinea
Guinea Bissau
Guyana
Haiti
Heard Island and Mcdonald Islands
Holy See (Vatican City State)
Iran
Iraq
Ivory Coast (Côte d'Ivoire)
Kiribati
Kosovo
Kyrgyzstan
Lao People's Democratic Republic
Lebanon
Liberia
Libya
Macao
Malawi
Mali
Marshall Islands
Martinique
Mauritania
Mayotte
Micronesia, Federated States of
Montserrat
Myanmar
Nauru
New Caledonia
Niger
Niue
Norfolk Island
North Korea
Northern Mariana Islands
Palau
Palestinian Territory
Papua New Guinea
Pitcairn
Puerto Rico
Rwanda
Saint Barthelemy

Saint Helena
Saint Kitts and Nevis
Saint Lucia
Saint Martin
Saint Pierre and Miquelon
Saint Vincent and the Grenadines
Sao Tome E Principe
Seychelles
Sint Maarten
Sierra Leone
Solomon Islands
Somalia
South Georgia and the South Sandwich Islands
Sudan (North and South)
Suriname
Svalbard and Jan Mayen
Syria
Tajikistan
Temporarily occupied territories of Ukraine
Timor Leste
Togo
Tokelau
Tonga
Turkmenistan
Turks and Caicos Islands
Tuvalu
United States of America
United States Minor Outlying Islands
US Virgin Islands
Uzbekistan
Vanuatu
Venezuela
Wallis and Futuna
West ern Sahara
Western Samoa
Yemen
Zimbabwe