

Black Ocean B.V.

**Business Plan
2026 - 2028**

Version: 1.1
Date: 04 February 2026

Confidential - For regulatory and banking/compliance purposes

Table of Contents

The following section list is provided for navigation purposes.

1. Executive Summary;
 2. Company Overview and Legal Structure;
 3. Business Activities and B2B Product Suite;
 4. Value Chain and Key Third Parties;
 5. Target Market and Commercial Strategy;
 6. Operations and Delivery Model;
 7. Detailed Management Structure, Key Persons and Internal Controls;
 8. Compliance and Regulatory Framework;
 9. Risk Management;
 10. Financial Plan 2026 - 2028;
- Appendices.

1. Executive Summary

Black Ocean B.V. is a Curaçao incorporated private limited liability company established on 7 April 2020. The Company operates as a Business-to-Business (B2B) provider of remote gaming software and related managed services to gambling operators (e.g., online casino and sportsbook operators). Black Ocean's activities are designed to be fully aligned with the requirements applicable to CGA-licensed B2B suppliers under the Landsverordening op de kansspelen (LOK) and related policies, procedures and guidance issued by the Curaçao Gaming Authority (CGA).

The Company's core commercial proposition is the provision of a modular iGaming platform (casino and sportsbook), including integrations to game content, payment methods and back-office tools such as CRM and reporting. Black Ocean leases the core platform software from Elsirel Ltd (Cyprus) and provides it to business clients under commercial sublicensing and service agreements, complemented by implementation, support, compliance and processing services.

- License scope: B2B game supplier / platform provider. Black Ocean does not offer player-facing gambling services and does not accept bets from players.
- Client base: regulated or otherwise authorised gambling operators in target markets (initial focus on LatAm and selected African markets), subject to a structured onboarding and due diligence process.
- Revenue model: a combination of setup/managed service fees and a revenue share linked to client Gross Gaming Revenue (GGR), plus fees for additional services and integrations.
- Operational approach: controlled platform onboarding, clear service ownership model, robust security and incident management, and an embedded compliance function covering AML/CFT, sanctions and regulatory reporting obligations applicable to the Company.

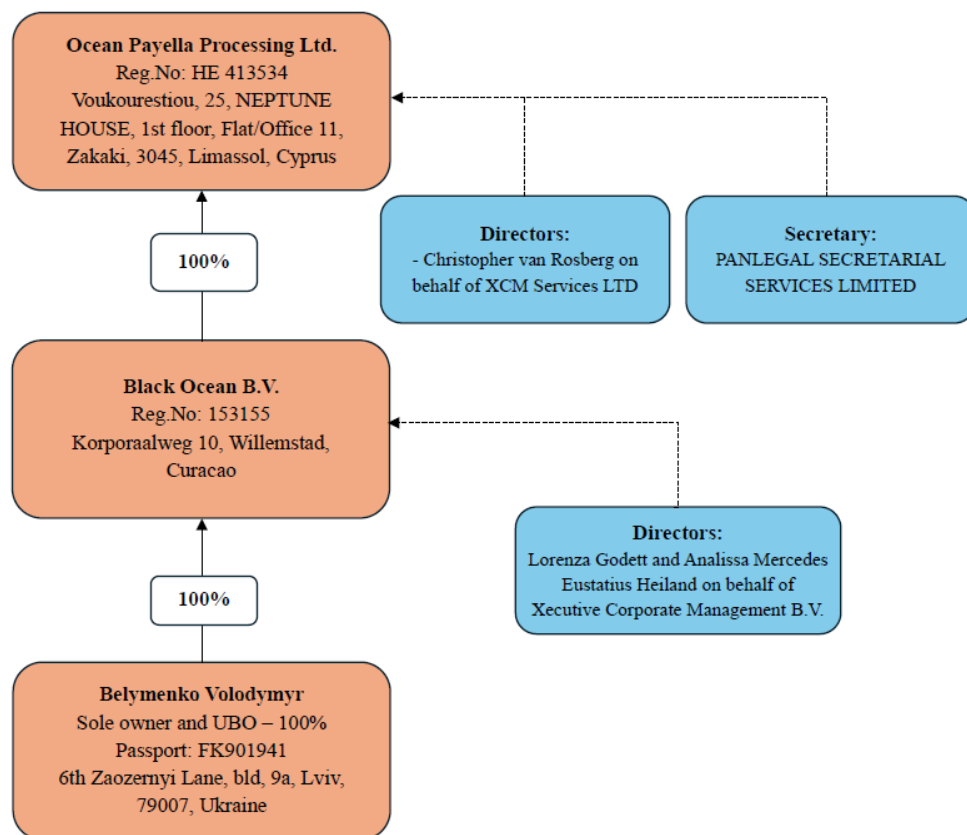
This Business Plan covers the period 2026 - 2028 and describes the Company's business activities, operating model, value chain, management structure, internal controls, compliance framework and financial projections.

2. Company Overview and Legal Structure

Black Ocean B.V. is incorporated in Curaçao as a private limited liability company (Besloten Vennootschap – B.V.). The Company's place of effective management and regulatory supervision is Curaçao.

Ownership and control:

- Sole Shareholder and Ultimate Beneficial Owner (UBO): **Mr. Volodymyr Belymenko**.
- Statutory / local director and official representative in Curaçao: **Xecutive Corporate Management B.V.**.



The Company maintains its regulatory relationship with the CGA via the CGA Portal and will ensure that corporate information, ownership information, key person appointments and material changes are accurately reflected in the CGA's records at all times.

Domains and branding: As a B2B license holder, Black Ocean will display the CGA B2B (Blue) authorisation seal only on its corporate website (<https://atlaslive.tech/>), which must correspond to the corporate website registered in the Organisation Details section of the CGA Portal. The Company will not use the CGA seal on any player-facing domain, and it will not operate player-facing domains under the B2B license.

3. Business Activities and B2B Product Suite

Black Ocean provides remote gaming software and related managed services to third-party gambling operators. The Company's offering is designed to support operators in launching and operating online casino and sportsbook products, while enabling operators to maintain their own player-facing regulatory and commercial responsibilities.

3.1. Scope of activities (B2B supplier)

- Provision of a modular iGaming platform (casino and sportsbook) through controlled integrations (e.g., iframe or API-based integration options).
- Provision of back-office tools including CRM, bonus engine, content management capabilities and reporting/analytics.
- Integration management with game service providers (aggregators / game manufacturers) and with payment method providers, as requested by clients.
- Ongoing technical support, maintenance, and incident response for the platform components under agreed service levels.
- Optional managed services: operational support to clients on configuration, risk controls, reporting dashboards and compliance tooling integration.

3.2. Platform components (high-level)

- Sportsbook integration - rapid integration for clients without a sportsbook or seeking to improve an existing offering.
- Casino aggregation - access to 5,000+ casino games (including live games), virtual sports and other content depending on client configuration and commercial agreements with content providers.
- CRM and bonus engine - proprietary CRM functions enabling segmentation, triggers, campaign automation and multi-channel communications.
- Payment methods integration - access to a wide range of payment methods (including crypto) via integrations, subject to client PSP relationships and applicable regulatory constraints.
- Business analytics - configurable reporting using multiple metrics and filters; dashboards and scheduled reporting for client stakeholders.

Black Ocean's service design is based on a clear separation of responsibilities: the client operator remains responsible for player-facing conduct, player funds, responsible gaming, KYC/AML for players, complaints handling and market access decisions; Black Ocean is

responsible for the availability, integrity and security of the supplied software components and for the performance of its own regulatory obligations as a Curaçao licensee.

Black Ocean does not open or manage player accounts, does not process player deposits/withdrawals in its own name, and does not hold player funds. Any payment processing is performed by the client operator and its appointed payment service providers.

4. Value Chain and Key Third Parties

Black Ocean uses a controlled value chain where critical components are provided under contract and are subject to due diligence, service level agreements and ongoing oversight.

Key third-party relationships include:

- Core platform licensor: Elsirel Ltd (Cyprus) - platform software is leased and provided onward to Black Ocean's clients under commercial arrangements. Platform software is leased from Elsirel Ltd starting August 2022.
- Game content suppliers / aggregators: third-party game providers and aggregators (selected based on reputation, licensing where applicable, security, and commercial fit).
- Payment method providers / hubs: integrations to payment service providers (PSPs) and/or technical hubs enabling multiple payment methods; clients contract with PSPs unless otherwise agreed.
- Infrastructure / hosting providers: Continent 8 Technologies Limited - cloud and data centre providers used to host and operate platform services, subject to information security and resilience requirements.
- Professional service providers: legal, accounting, audit and corporate services in Curaçao.

The Company maintains a third-party risk management process covering onboarding due diligence, contractual controls, access control, performance monitoring and exit/contingency planning for critical suppliers.

5. Target Market and Commercial Strategy

Black Ocean's primary customer segment is gambling operators seeking a reliable, scalable platform and rapid content/payment integrations. The initial commercial focus is on partners operating in LatAm and selected African markets, with a disciplined approach to jurisdictional risk and client acceptance.

5.1. Client onboarding and acceptance (B2B customer due diligence)

Prior to providing services, Black Ocean conducts risk-based due diligence on prospective clients and their key stakeholders, to ensure that business relationships are established only with suitable counterparties. The due diligence process includes, where applicable:

- Verification of the client's corporate identity, ownership and control, including UBO information.
- Assessment of the client's licensing and authorisation status in its target markets and confirmation that the intended use of the platform is lawful.
- Sanctions and PEP screening of client entities and relevant individuals.
- Assessment of AML/CFT controls and operational integrity (high-level review), with enhanced due diligence for higher-risk counterparties.
- Commercial and reputational review (open-source checks, adverse media).

5.2. Commercial model and pricing

The Company's commercial model is structured around:

- (i) implementation and managed service fees, and
- (ii) revenue share components linked to client GGR.

Additional fees may apply for bespoke integrations, localisation, reporting enhancements, and operational support packages. Fees are documented in client agreements and invoiced in accordance with Curaçao corporate and tax requirements.

6. Operations and Delivery Model

6.1. Implementation and onboarding lifecycle

- Contracting and scope definition (platform modules, content, payments, reporting, SLAs).
- Technical onboarding: integration design, security review, configuration of environments and access roles.
- Acceptance testing: functional, security and reporting checks; go-live approval.
- Launch support: heightened monitoring during initial operation period.
- Steady state operations: support, maintenance, change management and periodic service reviews.

6.2. Service management, support and incident handling

Black Ocean operates a service management framework to ensure continuity, integrity and traceability. Incidents impacting the security, availability or integrity of supplied services are recorded, triaged and resolved in accordance with defined procedures. Where an incident qualifies as a reportable event under the LOK and/or license conditions, Black Ocean will report it to the CGA via the Portal without delay and within the required timeframes (within twenty-four hours of an incident), and will provide follow-up reporting until closure.

6.3. Change management and access control

- Controlled release process for platform changes (risk assessment, approvals, testing and rollback planning).
- Role-based access controls, least-privilege access, strong authentication, and privileged access monitoring.
- Segregation of duties between development, deployment and production operations where applicable.
- Audit logging for critical system actions, configuration changes and administrative access.

7. Detailed Management Structure, Key Persons and Internal Controls

Black Ocean maintains a management structure that clearly allocates responsibilities, provides effective oversight and ensures that key functions are performed independently where required. The structure below identifies all key persons and describes responsibilities and controls.

7.1. Management and key persons (as notified to CGA)

Role	Name / Entity	Core responsibilities	Key controls	Oversight
Ultimate Beneficial Owner (UBO)	Volodymyr Belymenko	Ultimate ownership; Ensure the company has adequate financial resources to operate its business; Approve the overall risk appetite.	Approval of governance structure; Approval of strategic plan and annual budget.	Oversight of the Board or senior management; Periodic review of management reports.
Chief Executive Officer (CEO)	Volodymyr Hlynchak	Establishment and enforcement of internal policies and procedures; Clear reporting lines for AML and Compliance, Finance, and Technology; Approval of agreements (e.g., clients, suppliers); Ensuring staff competency and training.	Establishment and enforcement of internal policies and procedures; Clear reporting lines for AML and Compliance, Finance, and Technology; Approval of agreements (e.g., clients, suppliers); Ensuring staff competency and training.	Oversight of operational, compliance, and financial performance; Regular review of risk assessments and compliance reports; Escalation of material incidents to the UBO where required.

Chief Financial Officer (CFO)	Oleksii Hrebeshchuk	Accurate and timely financial statements; Controls over payments, revenue flows, and expense management; Monitoring of transactions for financial irregularities.	Accurate and timely financial statements; Controls over payments, revenue flows, and expense management; Monitoring of transactions for financial irregularities.	Oversee accounting, budgeting, and financial reporting; Oversight of audits; Reporting financial risks and irregularities to CEO.
Chief Technology Officer (CTO)	Oleksandr Koliush	Client due diligence for customers (including Sanctions and PEP screening); Ongoing transaction monitoring; Record-keeping and reporting mechanisms; Regulatory gap analysis and implementation of corrective actions.	Secure development and deployment processes; Access controls, change management and logging; System uptime, disaster recovery, and business continuity planning.	Oversight of technical risks, including cybersecurity; Reporting on system performance and incidents.

7.2. Operational teams and outsourced resources

Beyond the above key persons, Black Ocean uses a mix of internal staff and specialised third-party resources for development, support, sales, integration and operational functions. Where third parties are used, the Company maintains contractual controls, confidentiality obligations, access restrictions and performance monitoring.

8. Compliance and Regulatory Framework

Black Ocean maintains a compliance framework proportionate to its activities as a B2B supplier and aligned with applicable Curaçao laws, CGA license conditions and published guidance. The compliance framework is designed to be practical, risk-based and auditable.

8.1. Regulatory governance and reporting

- All regulatory communications with the CGA are handled via the CGA Portal ticketing system, with responsibility assigned to the Local Director and the Compliance function.
- Reportable incidents (including security breaches, significant system failures and fraud/criminal behaviour involving key persons or staff) are reported via the Portal within required timeframes.
- The Company maintains complete and accurate corporate, ownership and key person information in the Portal, and updates it without delay when changes occur.

8.2. AML/CFT, sanctions and financial crime controls

The Company adopts and maintains an AML Policy consistent with CGA expectations for license applicants and holders. The policy is approved by management, reviewed at least annually and updated upon material regulatory or business changes. Key elements include:

- Business Risk Assessment (BRA) covering ML/TF/FP risks by products/services, customer types, delivery channels and geographies, and defining risk appetite.
- Customer Risk Assessment (CRA) and Customer Acceptance Policy (CAP) for onboarding of B2B clients and relevant persons; enhanced due diligence for higher-risk cases.
- Sanctions and PEP screening, including screening against UN and EU sanctions lists, and procedures for escalation, freezing and reporting where required.
- Ongoing monitoring of business relationships and transactions, including detection of unusual patterns and escalation procedures.
- Reporting of unusual transactions to the Curaçao FIU where applicable, and strict compliance with the prohibition of tipping-off.
- Record keeping for CDD information, contracts, screening results, and transaction data for the applicable retention period.
- AML training for relevant staff and contractors, including onboarding training and periodic refreshers.

Although Black Ocean is not a player-facing operator, it recognises that B2B suppliers can be exposed to financial crime risk through their clients. Accordingly, the Company applies risk-based due diligence and monitoring to B2B counterparties and maintains contractual provisions requiring clients to operate in compliance with applicable laws, including AML/CFT and sanctions requirements.

8.3. Data protection, information security and resilience

- Information Security Management: security-by-design, secure development practices, vulnerability management and penetration testing where appropriate.
- Data governance and privacy: data minimisation, access restriction, encryption in transit and at rest where feasible, and controlled cross-border transfers.
- Business continuity and disaster recovery planning for critical systems and client support operations.
- Incident response plan with defined escalation and communication procedures, including client notifications and regulatory reporting where required.

8.4. Local substance and Curaçao presence

Black Ocean maintains a Curaçao presence consistent with local substance requirements under Article 5.12 of the LOK and the CGA's published guidance. The Company notes that the Minister of Justice has granted a general extension, and operators are not required to meet the local substance obligation under Article 5.12 before 1 April 2027. Black Ocean will nevertheless develop and maintain Curaçao substance in a timely manner and ensure full compliance by the applicable statutory deadline.

- Maintaining dedicated office facilities in Curaçao suitable for the licensed business activities.
- Ensuring that required key persons are engaged full-time and registered in Curaçao in line with applicable timelines.
- Maintaining documented engagement arrangements (employment or contractual) and evidence of registration and office availability.

8.5. Change of control and key person changes

Black Ocean applies a strict prior-approval approach to any changes in ownership or control structure, in line with CGA procedures. No share transfer or appointment of a new statutory director is completed until the CGA has expressly approved the change. The Company will submit required corporate and personal documentation via the CGA Portal and open a support ticket for processing.

9. Risk Management

The Company applies a risk management approach that identifies, assesses and mitigates key risks relevant to a B2B platform supplier.

Key risk categories and mitigation measures include:

- **Regulatory risk:** Regular compliance monitoring, policy maintenance, change management controls, timely portal reporting and governance oversight.
- **Third-party/vendor risk:** Due diligence, contractual SLAs, security requirements, performance monitoring and contingency planning.
- **Technology and cybersecurity risk:** Access control, secure SDLC, monitoring, incident response, backups and resilience testing.
- **AML/financial crime risk:** Risk-based client due diligence, sanctions/PEP screening, monitoring and escalation/reporting procedures.
- **Operational risk:** Documented processes, segregation of duties, training, and quality assurance for integrations and releases.
- **Reputational risk:** Client acceptance standards, responsible marketing (B2B), transparent governance and prompt incident communication.
- **Financial risk:** Budgeting and forecasting, treasury controls, cost management, and diversified client pipeline.

10. Financial Plan 2026 - 2028

The financial projections for 2026 - 2028 are based on the Company's current client pipeline, expected client GGR volumes, contracted and anticipated revenue share rates, and cost assumptions for content providers and software/license fees. Amounts below are presented in EUR '000.

In 2026 the Company forecasts Total Revenue of EUR 49,631k and Net Ordinary Profit of EUR 2,488k. For 2027 the forecast is Total Revenue EUR 56,696k and Net Ordinary Profit EUR 3,814k; for 2028 Total Revenue EUR 62,032k and Net Ordinary Profit EUR 5,792k.

10.1. Key financial drivers

- Revenue from sportsbook and casino is linked to a share of client GGR, complemented by fees for other services and integrations.
- Cost of goods sold largely consists of game content provider fees and software/license/server fees, reflecting the Company's position in the value chain.
- Operating expenses include professional fees and other operating costs required to maintain regulated operations and Curaçao corporate substance.

10.2. Black Ocean Financial information and plan

Black Ocean B.V.

Statement of profit & loss

Amounts in EUR '000

	<i>actual</i>	<i>actual</i>	<i>plan</i>	<i>plan</i>	<i>plan</i>	<i>plan</i>	<i>plan</i>
	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL	TOTAL
	2022	2023	2024	2025	2026	2027	2028
Clients' operations							
<i>GGR Sportbook</i>	<i>910</i>	<i>12,900</i>	<i>4,880</i>	<i>5,862</i>	<i>6,300</i>	<i>7,000</i>	<i>7,500</i>
<i>GGR Casino</i>	<i>20,665</i>	<i>205,400</i>	<i>414,544</i>	<i>372,360</i>	<i>417,043</i>	<i>479,600</i>	<i>527,560</i>
Revenue Sportbook	109	1,417	596	703	756	840	900
Revenue Casino	2,962	28,363	38,384	37,236	45,875	52,756	58,032
Other services	121	2,107	1,327	2,600	3,000	3,100	3,100
Total Revenue	3,192	31,887	40,307	40,539	49,631	56,696	62,032

Casino games providers' Fee	2,148	20,025	23,305	20,480	29,193	33,572	36,929
Software, license and server fees	365	-	15,252	18,000	15,600	16,800	16,800
Total COGS	2,513	20,025	38,557	38,480	44,793	50,372	53,729
Gross Profit	679	11,862	1,750	2,060	4,838	6,324	8,302
Professional fees	224	921	780	850	900	950	950
Other expenses	33	152	1,755	1,250	1,450	1,560	1,560
Operating Expense	257	1,073	2,535	2,100	2,350	2,510	2,510
Net Ordinary Profit	422	10,789	(785)	(40)	2,488	3,814	5,792

Appendices

Appendix 1 - Policy and procedure suite (high-level)

The Company maintains and will continue to maintain the following core documents, proportionate to its B2B activities:

- AML Policy and Business Risk Assessment (BRA); Client due diligence procedures; sanctions/PEP procedures; FIU reporting procedure.
- Compliance Policy and Regulatory Reporting Procedure (including incident reporting via the CGA Portal).
- Information Security Policy, Incident Response Plan, Access Control Standard, Change Management Procedure.
- Third-Party/Vendor Due Diligence and Outsourcing Procedure.
- Business Continuity and Disaster Recovery Plan.
- Data Retention and Record Keeping Policy.
- Conflicts of Interest Policy.
- Change of Control Procedure (internal) aligned with CGA prior-approval requirements.

Appendix 2 - Glossary

- **B2B**: Business-to-Business.
- **B2C**: Business-to-Consumer (player-facing operator).
- **CGA**: Curaçao Gaming Authority.
- **CDD**: Customer Due Diligence.
- **GGR**: Gross Gaming Revenue.
- **LOK**: Landsverordening op de kansspelen (National Ordinance on Games of Chance).
- **PEP**: Politically Exposed Person.
- **PSP**: Payment Service Provider.
- **SLA**: Software License Agreement.