

Portobahis

Website Functional Description

Operational Manual · Red Lane B.V. · portobahis684.com

Document Overview

Website Functional Description

This document is the functional description of the player-facing website, portobahis.com. It gives a structured, screen-by-screen description of the player-facing experience.

Document Control

Field	Value
Document title	Website Functional Description
Document type	Functional description, player-facing platform
Version	1.0
Revision date	2026-05-12
Status	Released
Confidentiality classification	Internal — Restricted Distribution
Operator	Red Lane B.V.
Legal address	Schottegatweg Oost 10, Unit 1-9 Bon Bini Business Center, Willemstad, Curaçao
Operating licenses	Curaçao Gaming Authority — Gaming Licence No. OGL/2024/1065/0847
Website	https://portobahis684.com/
Operations	24 hours a day, 7 days a week (except scheduled maintenance)
Support email	support@portobahis684.com
Disputes / claims email	support@portobahis684.com
Document language	English
Prepared by	Portobahis Operations
Approved by	Red Lane Management

Revision history

Version	Date	Author	Summary
1.0	2026-05-12	Portobahis Operations	Initial issue. Establishes the functional description of the player-facing website.

Scope

The document describes the player-facing website at <https://portobahis684.com/> — what visitors and registered players see, the screens they can use, the actions they can take, and the controls that protect them. It does not describe the internal administrative back-office, the operator's deployment infrastructure, or the internal logic of third-party providers integrated into the platform.

Structure

The document is organized into the following sections covering the player-facing surface of the website.

Contents

1. General Description of the Website
2. Main Sections and Interface of the Website
3. Registration and Authorization
4. User Profile
5. Game Categories and Search
6. Promotions and VIP Program
7. Customer Support (Support Services)
8. Language and Localisation
9. Security and Data Protection
10. Platform Technical Specifications
11. Outcome Determination / RNG
12. RNG Implementation Standards
13. Testing Procedures Implemented by Providers
14. Third-Party Certification
15. Data Centre and Physical Security
16. GDPR Compliance and Data Protection Principles
17. Secure Deletion (as part of data retention)
18. Elements of Visual Representation
19. Terms and Conditions
20. File Contents and Digital Record Management Framework

Method

The descriptions were prepared from structured analysis of the live website. Where a behaviour is configured server-side and is not directly observable from the player's perspective, the document states this explicitly.

1. General Description of the Website

1.1 Purpose

Portobahis is an online gambling website operated by **Red Lane B.V.**, a company duly incorporated under the laws of Curaçao and registered with the Commercial Register of the Curaçao Chamber of Commerce & Industry under registration number **149962**.

The Company's registered office is located at:

Schottegatweg Oost 10, Unit 1-9
Bon Bini Business Center
Willemstad, Curaçao
Dutch Caribbean

Red Lane B.V. is authorised by the **Curaçao Gaming Authority (CGA)** to organise and offer games of chance under **Gaming Licence No. OGL/2024/1065/0847**, and conducts its operations in accordance with the applicable provisions of the **National Ordinance on Games of Chance (LOK)**, the regulations, directives, and licensing requirements issued by the Curaçao Gaming Authority, and all other applicable laws and regulatory obligations governing online gaming activities in Curaçao.

The Portobahis website is a secure, mobile-responsive online gaming platform that provides players with a comprehensive range of gambling products and services through a single integrated website.

The platform offers, among others:

- Online Casino Games
- Live Casino Games
- Sportsbook and Live Sports Betting
- Virtual Sports
- Esports Betting

1.2 Target audience

The website serves:

- Adults of permitted age:
 - Turkish Citizens — 25 years of age and above
- Verified account holders with completed identity verification (KYC) who have unrestricted access to deposit, play, and withdraw.
- Visitors browsing the public catalogue prior to registration. Public visitors may inspect the game catalogue and read promotional and informational pages; they cannot place wagers without registering.

The website is **not** intended for:

- Persons below the age limits set out above.
- Persons who have self-excluded.

- Persons placed on a register of persons restricted from gambling activity (where such a register applies under local legislation).
- Persons resident in jurisdictions excluded by the operator's licence or local law.

These exclusions are enforced by the operator through:

- **Identity verification (KYC)** built on two mandatory pillars: a government-issued identity document (national ID card, passport, or driving licence) and a live face check in which a real-time selfie is biometrically matched against the photograph on the document under a Liveness Check that confirms a live human being is present (and not a photograph, screen, video, or mask). The verification is described in detail in §3.3.

1.3 High-level capability summary

Capability area	What the website provides
Casino	Slots, live casino, table games, virtual sports, crash and instant games, favourites
Sportsbook	Pre-match sports betting through an integrated sportsbook provider
Live sport	In-play sports betting through an integrated live-sport provider
Esports	Esports event betting through an integrated esports provider
Account management	Registration, login, password reset, profile editing, document upload, change-password, session history
Cashier	Deposit and withdrawal through multiple payment-service providers (card, bank, e-wallet, crypto)
Bonuses	Bonus claim, bonus history, free-spin history, cashback, redeem
VIP	VIP loyalty programme with tier-based benefits
Promotions	Marketing promotions and promotion-detail pages
Responsible gambling	Self-exclusion, cooling-off period, account limitation, deposit and loss limits
Customer support	Live in-app chat, support email, integrated help
Realtime	Live online-player counter, live bets feed
Mobile	Responsive layout for tablet and mobile browsers

1.4 Technical platform — high level

The website is a modern single-page web application. The technical stack is operator-internal and is documented in the operator's policy framework. For the purposes of this functional description, the relevant operational facts are:

Aspect	Behaviour
Hosting	Production website at https://portobahis684.com/ , delivered over HTTPS exclusively
Devices	Desktop, tablet, and mobile (responsive web)
Realtime	Live updates for online-player count, live bets stream, and notifications

Game launching	Casino and live-casino games launch in an in-page game frame; provider game-rounds run inside the frame
Sportsbook embedding	Sportsbook, live-sport, and esports surfaces are embedded as live in-page surfaces from the integrated provider
Identity verification	KYC document collection and review through an integrated identity-verification service
Payments	Deposit and withdrawal through multiple PSPs (card processors, bank transfer, e-wallet providers, cryptocurrency gateways)
Customer support	In-app live chat through an integrated support service

1.5 Public vs. authenticated experience

The website is designed so a visitor can explore the catalogue, learn about the brand, and decide to register; once registered and verified, the same continuous experience extends to deposits, play, withdrawals, and self-service account management.

Surface	Public visitor	Authenticated player
Browse game catalogue	✓	✓
Browse providers	✓	✓
View promotion details	✓	✓
View VIP programme details	✓	✓
Switch interface language	✓	✓
Open live-chat support	✓	✓
Register a new account	✓	—
Sign in to existing account	✓	—
Recover forgotten password	✓	—
Place a wager (casino, sport)	—	✓ (verified)
Deposit funds	—	✓ (verified)
Withdraw funds	—	✓ (verified)
Manage account settings	—	✓
Upload KYC documents	—	✓
Claim a bonus	—	✓
View transaction history	—	✓
Set responsible-gambling limits	—	✓
Self-exclude	—	✓

1.6 Operating principles

The platform operates on the following principles, each elaborated in the relevant section below:

1. **Verified play** — only verified accounts may deposit, wager and withdraw at full capability. The KYC verification flow is integrated directly into the registration journey.
2. **Multi-provider integration** — sportsbook, live-sport, esports, casino, and payment functions are delivered through integrated providers, with the website acting as the operator-side surface.
3. **Player protection by design** — responsible-gambling tools (limits, cooling-off, self-exclusion) are first-class features of the account dashboard.
4. **Transparent account history** — every transaction, bet, bonus, and session is reflected in the player's account dashboard.
5. **Live support** — a live-chat support channel is reachable from every page of the website.

1.7 Where the rest of the document goes

The remainder of this document describes each functional area of the website in detail. Section 2 covers the screens and navigation. Sections 3–10 cover the functional themes of the player-facing platform — registration and authorisation, the user profile, game categories and search, promotions and the VIP programme, customer support, the language switcher and multilingual support, security and data protection, and the platform's technical specifications. Sections 11–20 cover outcome determination and RNG, testing and certification frameworks, data centre and physical security, GDPR data protection, secure deletion, visual representation elements, terms and conditions, and the digital record management framework.

2. Main Sections and Interface of the Website

This section catalogues the public-facing screens of the website and the interface elements that appear across all of them. Each subsection identifies a single screen or a closely-related group of screens, with the URL paths that lead to them.

2.1 Global interface elements

Every screen on the website carries a consistent set of global elements:

Element	Position	Function
Header / brand bar	Top of every page	Brand logo (links to home), primary navigation, search affordance, language switcher, sign-in / register actions (for visitors), or balance + account menu (for authenticated players)
Primary navigation	Top header	Casino, Live Casino, Sportsbook, Live Sport, Esport, Promotions, VIP
Search	Top header	Game-catalogue search; opens an overlay with type-ahead results
Language switcher	Top header	Opens a list of available languages; choice persists
Balance & account menu	Top header (authenticated)	Shows current account balance with quick links to Deposit, Withdraw, Profile, Logout
Live chat launcher	Bottom-right floating button	Opens the live-chat customer-support window
Footer	Bottom of every page	Operator identity, licence numbers, age-restriction notice, responsible-gambling notices, secondary navigation (terms, privacy, support pages), payment-method icons, links to social channels
Cookie / age banner	First visit	Cookie-consent and age-confirmation notice, dismissable per session
Online-player counter	Header or footer	Live count of currently-online players (updates via realtime channel)

The interface is **mobile-responsive**: on tablet and mobile widths the primary navigation collapses into a hamburger menu and the dashboard layouts re-flow into single-column views. Mobile-optimised game tiles and game-frame sizes are applied at smaller breakpoints.

2.2 Home

URL	/
Audience	All visitors

The Home screen is the principal landing page. It carries:

- A hero slider showing campaign creatives, promotions, and brand messages.
- A short, hand-curated "top games" row.
- Featured categories (slots / live casino / table games / sportsbook teaser).
- A providers row with logos of major content partners.
- A promotions strip linking into the Promotions section.
- A "live winners" strip showing recent significant wins (real-time updates).

Login, Registration, and Forgot-password are reachable from the Home screen as overlay dialogs that do not navigate away — the URL changes to `/login`, `/register`, and `/forgot` respectively while the home content remains in the background.

2.3 Casino lobby

URL	<code>/slots</code> , <code>/browse-slots</code> , <code>/games</code>
Audience	All visitors

The casino lobby presents the slot-game catalogue, categorised by:

- Featured / Popular / New / Most-played
- Game theme (Fruits, Mythology, Adventure, Branded, ...)
- Volatility (low / medium / high)
- Provider (filterable from the provider list)
- Bonus features (free spins, multipliers, jackpots)

2.4 Live Casino

URL	<code>/live-casino</code> , <code>/browse-live</code>
Audience	All visitors

The live-casino lobby surfaces live-dealer tables (roulette, blackjack, baccarat, game shows) from the integrated live-casino providers.

2.5 Sportsbook

URL	<code>/sportsbook</code>
Audience	All visitors

The sportsbook lobby embeds the active sportsbook provider's catalogue. The website is designed to integrate with a sportsbook provider; the embedded experience offers sport navigation, featured events, betslip with single/accumulator/system bet construction, cashout (where supported), and bet history.

2.6 Live Sport

URL	/live-sport , /livesport
Audience	All visitors

The live-sport lobby embeds the in-play sports surface from the integrated provider. Live-sport offers in-play wagering with constantly-updating odds and event states.

2.7 Esports

URL	/esport
Audience	All visitors

The esports surface is provided through an integrated esports provider. Markets cover the principal competitive titles (e.g. CS, DOTA, LoL, Valorant), with both pre-match and live in-play markets.

2.8 Game providers

URL	/providers , /provider/:id
Audience	All visitors

A directory of integrated game providers, with a logo grid and a per-provider page listing every game from that provider.

2.9 Promotions

URL	/promotions , /promotions/:slug
Audience	All visitors

The promotions index lists active marketing offers. Each promotion has a detail page with image, title, body, terms & conditions, eligibility (customer-group targeting), start and end dates, and a call-to-action (claim / opt-in for authenticated players, register for visitors).

2.10 VIP

URL	/vip
Audience	All visitors (programme overview); authenticated players see their own tier

The VIP page describes the loyalty programme — tier names, benefits at each tier, progression criteria.

2.11 Account dashboard (authenticated)

URL	/account/*
Audience	Authenticated players

The account dashboard is the player's personal back-office. It is described in detail in section 4. The principal sub-screens are:

Sub-screen	URL
Account home	/account
Settings	/account/settings
Security (password change)	/account/security
Verification (KYC)	/account/verification
Sessions history	/account/sessions
Financial transactions	/account/finance
Game transactions	/account/game-transactions
Sportsbook history	/account/sport-history
Bonus history	/account/bonus-history
Free-spin history	/account/free-spin-history
VIP programme	/account/vip
Account limitation	/account/account-limitation
Cooling-off period	/account/cooling-off
Self-exclusion	/account/self-exclusion

2.12 Cashier

The cashier is presented as a modal layer on top of any screen — players can deposit or withdraw without leaving the page they were on. The cashier covers deposits, withdrawals, saved payment instruments, and pending/completed transaction status.

2.13 Search

A dedicated search affordance opens a type-ahead overlay. The search index covers game names, provider names, and game categories. Results are returned in real time as the player types.

2.14 Game launch (Play Game)

URL	/play/:gameId
Audience	Verified authenticated players (and optionally demo mode for unauthenticated visitors)

Clicking a game tile opens the game launcher. The game frame embeds the provider's game client. The player's main wallet, balance, and session timer remain visible alongside the frame on desktop.

2.15 Standard pages

URL	/page/:slug
Audience	All visitors

Static CMS-style pages — terms and conditions, privacy policy, responsible gambling, AML policy, cookie policy, about us, contact, help. Linked from the footer.

2.16 Not found

A friendly 404 page with a return-to-home link for any unmatched path.

2.17 Navigation and information architecture

The navigation reflects a single, unified product story: visitors enter at Home, browse categories from the primary navigation, drill into game lobbies or sportsbook surfaces, optionally drill into promotions or the VIP page, and either register / sign in to play, or open live chat for support. Once authenticated, the account dashboard becomes the destination for personal account management, history, and responsible-gambling controls. The live-chat surface described in Section 7 is reachable from every page of the website.

3. Registration and Authorization

This section describes how a visitor becomes a registered player, how an existing player signs in, how forgotten credentials are recovered, and how identity verification (KYC) is integrated into the journey.

3.1 Registration

3.1.1 Where it is reached

The registration dialog is reached from the Register button in the top navigation, the Register call-to-action on the Home page hero, the URL `/register`, and the promotion-detail pages where a "Register to claim" call-to-action appears to visitors.

3.1.2 Age eligibility

In line with applicable Georgian gambling legislation, the right to register on the website and to place wagers is restricted by age:

- Georgian citizens — 25 years of age and above.
- Foreign nationals — 18 years of age and above.

Age eligibility is confirmed during identity verification (KYC) — the player's date of birth is extracted from the identity document. A registration is treated as conditional until verification succeeds.

3.1.3 What the player provides at registration

Fields collected on the registration form:

Field	Type	Purpose
Username	text	Sign-in identifier
Email address	email	Account contact, recovery, transactional and (where opted in) marketing communications
Mobile phone number	phone	Account contact, recovery, SMS verification
Password	password	Authentication credential
Currency	dropdown	Wallet currency
Marketing consent	checkbox	Opt-in for promotional communications
Terms-and-conditions acceptance	checkbox	Explicit acceptance of the platform's Rules, the Personal Information Management policy, and (by implication) the AML and Data Protection policies

Fields captured automatically during verification (not entered manually): First name, Surname, Father's name, Date of birth, Place of birth, Citizenship, Country of residence, Personal identification number, Document type / issuing country / authority / issue date and expiry, Sex/gender.

3.1.4 Field requirements

- The form validates client-side for format (email, phone) and server-side for uniqueness (username, email, phone).
- The password is validated against the operator's complexity policy.
- Marketing consent is opt-in.
- Terms acceptance is mandatory to complete registration.
- The player is expressly warned that the username and password must not be shared with third parties.

3.1.5 Anti-bot protection

The registration form is protected by an invisible bot-protection challenge that runs silently on submit.

3.1.6 What happens on submit

1. The form is validated client-side; any invalid field is highlighted.
2. The data is sent to the back end over HTTPS.
3. The back end verifies uniqueness (username, email, phone), validates the password against complexity rules, checks the anti-bot signal, and checks for IP-blacklist / country-restriction matches.
4. On success, the account is created in `pending_verification` status. The new player is signed in automatically and receives an on-screen welcome, a welcome email, and an SMS verification code.
5. The player is prompted to complete identity verification (KYC) before depositing.

3.1.7 One account per player

In line with the Account Management Policy, a player is entitled to a single account on the platform. Multiple accounts are detected by matching personal identification number, biometric match, payment-instrument overlap, device fingerprint, and other signals; on detection, all associated accounts are blocked and only the first-created account is retained.

3.1.8 Failure modes

Reason	Player-visible message
Field invalid (format)	Inline field error with the format expected
Duplicate username / email / phone	Translated message indicating the conflict
Password fails complexity	Translated message explaining the requirements
Bot-protection failed	Translated message; offer to retry
Country restricted	Translated message indicating the platform is not available in the visitor's location
IP blacklisted	Translated message; no detail given
Multi-account detected at verification	Translated message; the player is referred to support

3.2 SMS / phone verification

After registration the player is asked to verify their phone number by entering a one-time code sent via SMS.

Verification is mandatory before the player can deposit; retries are rate-limited; the code expires after a short window; a "resend code" option appears after a brief delay.

3.3 Identity verification (KYC)

Identity verification is the mandatory step that transitions an account from `pending_verification` to fully verified. Only fully-verified accounts may withdraw winnings, and (per operator policy) may be required to verify before depositing larger sums.

Verification is built on two mandatory pillars:

1. **An identity document** — the player presents a government-issued identity document (national identity card, passport, or driving licence) that bears a personal identification number and a photograph of the holder.
2. **A live face check (Liveness Check)** — the player captures a real-time selfie that is biometrically compared with the photograph on the identity document, while the system simultaneously verifies that a live human being (not a photograph, video, or mask) is present at the device.

3.3.1 Where KYC is collected

KYC is collected through a dedicated screen at `/account/verification`. The screen is also presented inline at the moment the player attempts an action that requires verification (for example, a first withdrawal).

3.3.2 KYC flow — ID card + face verification

KYC verification is performed through an integrated third-party identity-verification provider. The provider runs entirely inside the website (no external redirection to a different domain). The flow is automated end-to-end in the standard case; a manual review is initiated only where the automated checks raise a concern.

1. The website opens the verification dialog and requests an access token from the back end.
2. The verification provider's interface is rendered inside the website.
3. **Step A — Document capture.** The player chooses the document type — national identity card (default), passport, or driving licence. The player captures the front and back of the document.
4. **Step B — Live face capture.** The player captures a real-time selfie through the device camera under a Liveness Check that confirms a live human is present and biometrically compares the face against the document photograph.
5. **Step C — Automated verification.** The verification provider performs document authenticity checks (security-feature analysis, font and layout consistency, MRZ / barcode parsing), biometric face match, and liveness scoring.
6. The structured identification data is extracted from the document and recorded against the player's account.
7. The result is reported back to the operator's back end: **Approved**, **Pending review**, or **Rejected**.

3.3.3 Biometric data processing

The Liveness Check produces biometric data. The processing of biometric data is performed for the purpose of meeting the verification requirements of the applicable gambling legislation; the data is treated under the operator's Personal Information Management Policy and Data Protection Policy. Retention is limited to the period required by law.

3.3.4 Customer Due Diligence (CDD)

In line with the operator's Anti-Money-Laundering Policy and the requirements of the Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism, the EU Third Directive (26 October 2005), and FATF recommendations, every registration triggers a Customer Due Diligence (CDD) procedure performed by the operator's AML unit.

Clients are classified by risk level:

Risk level	Profile	Re-identification cadence
Low	Clients whose transactions are not suspicious from a money-laundering perspective	Every five years
High	Politically Exposed Persons (PEPs); non-commercial organisations; clients exhibiting unusual behaviour; clients about whom a Suspicious Transaction Report has been filed; clients linked to high-risk industries or sanctioned countries	Every year

3.3.5 Document policy

- Identity documents must be valid (not expired).
- Where the business relationship is resumed after an interruption, the client must be re-identified.
- Where verification cannot be completed, the business relationship is not initiated or is terminated.

3.4 Sign-in (login)

3.4.1 Where it is reached

The login dialog is reached from the Sign in button in the top navigation, the URL `/login`, and automatic redirection when an unauthenticated visitor attempts an authenticated action.

3.4.2 What the player provides

Stage 1 — credentials (username/email/phone + password). Stage 2 — second factor (optional, per account): TOTP code from an authenticator app, or SMS code.

3.4.3 Anti-bot protection

The login form is protected by the same anti-bot mechanism as registration.

3.4.4 What happens on submit

1. Credentials are validated client-side for non-emptiness only.
2. Credentials are sent to the back end over HTTPS.
3. The back end verifies the credentials, checks account state, checks if the source IP is blacklisted, and applies rate-limiting. **Three (3) consecutive unsuccessful sign-in attempts trigger automatic account logout** (see §9.3.2).
4. On success, a session is established.
5. On failure, a translated error is shown with no detail that could assist an attacker.

3.4.5 Persistent sign-in

The player can opt for "Remember me" at sign-in. Where enabled, the session token is persisted across browser restarts subject to a server-defined maximum lifetime.

3.4.6 Logout

Logout is reached from the account menu in the top header. Logging out invalidates the session both client-side and server-side.

3.4.7 Suspicious-activity reporting by the player

If the player observes suspicious activity on their account, they are required to change the password immediately and contact the operator. This obligation is part of the Account Management Policy.

3.5 Password recovery (Forgot password)

The forgot-password dialog is reached from a "Forgot password?" link in the login dialog or the URL `/forgot`.

Flow:

1. The player enters their registered email address (or, per operator policy, their username or phone).
2. A reset link / code is dispatched to the player's registered email (or SMS).
3. The player follows the link or enters the code on a reset screen.
4. The player is asked to choose a new password meeting the complexity policy.
5. On success, the player is signed in (or returned to the login dialog, per operator policy).
6. The password change is recorded in the player log and the account's session-history view; the player is also notified by email of the password change.

3.6 Account-state interactions

The state of the account at the moment of sign-in determines what the player can do. The principal states and their effect:

Account state	Sign-in allowed?	Effect
active	✓	Full access.
pending_verification	✓	Sign-in works; deposit and withdrawal may be restricted until KYC is completed.
id_verification	✓	Same as above; player is prompted to upload identity documents.
credit_card_verification	✓	Sign-in works; an additional verification step is presented before deposit.
cooling-off	✓ for read-only access	Sign-in shows account history but blocks deposit and play until the cooling-off period elapses.
self-excluded	—	Sign-in is rejected with a notice about the self-exclusion period.
locked	—	Sign-in is rejected. The player is invited to contact support.
dormant	per recovery flow	Account inactive for ≥ 1 year; the operator notifies the player and gives a reasonable window to resume activity before closure.
inactive	✓ on first sign-in attempt; activation flow	The account is re-activated if the player provides a valid credential set and (where required) completes any re-verification step.

deleted	—	Sign-in is rejected.
---------	---	----------------------

3.7 Pre-authentication geographic restrictions

Where the visitor's apparent country (determined from IP) is not on the operator's allowed-country list, the website displays a notice indicating the property is not available in their location. Registration and login are blocked from such locations regardless of the credentials offered.

3.8 Public-page experience for unauthenticated visitors

Unauthenticated visitors can browse the entire game catalogue (without launching games into real-money play), read promotions and the VIP page, read all static-page content, switch language, open live chat to ask questions, and initiate registration or sign-in. Visitors cannot place wagers, deposit, claim bonuses, see another user's data, or upload KYC documents.

4. User Profile

This section describes the authenticated player's personal area — the account dashboard — and the actions the player can take on their own data, money, history, and protection settings.

4.1 Where the profile is reached

The profile is reached from the account menu in the top header, the URL `/account` (and sub-screens at `/account/...`), and inline calls-to-action from elsewhere in the site.

4.2 Profile layout

The profile dashboard uses a two-column layout on desktop: Left navigation (list of all profile sub-screens; the active screen is highlighted) and Main content (the active sub-screen). On mobile the navigation collapses into a top-of-screen selector.

4.3 Sub-screens

#	Screen	URL	Function
4.4	Account home	<code>/account</code>	Personal information overview, edit identity data
4.5	Settings	<code>/account/settings</code>	Communication preferences, language, marketing opt-in
4.6	Security	<code>/account/security</code>	Change password, manage two-factor authentication
4.7	Verification (KYC)	<code>/account/verification</code>	Upload identity documents, see verification status
4.8	Sessions	<code>/account/sessions</code>	List of recent logins; end other sessions
4.9	Finance (financial transactions)	<code>/account/finance</code>	History of deposits and withdrawals
4.10	Game transactions	<code>/account/game-transactions</code>	History of casino game-rounds
4.11	Sport history	<code>/account/sport-history</code>	History of placed bets and their settlement
4.12	Bonus history	<code>/account/bonus-history</code>	History of bonuses received, redeemed, expired
4.13	Free-spin history	<code>/account/free-spin-history</code>	History of free-spin awards
4.14	VIP	<code>/account/vip</code>	Personal VIP tier, points, progress

4.15	Account limitation	/account/account-limitation	Set deposit / loss / wager / session limits
4.16	Cooling-off period	/account/cooling-off	Set a short responsible-gambling cooling-off
4.17	Self-exclusion	/account/self-exclusion	Self-exclude for a specified period

4.4 Account home

Displays the player's identity data and lets the player edit non-restricted fields. Restricted fields (those captured during KYC — first name, last name, date of birth, personal identification number) are read-only after verification; changes to these require contacting support and undergoing a re-verification step.

Editable fields typically include: Address, City, Postal code, Mobile phone (subject to SMS re-verification), Email (subject to email re-verification), Country of residence (read-only after KYC).

4.5 Settings

Display language, marketing email/SMS/push opt-in, newsletter subscriptions, cookie preferences, currency display preference.

4.6 Security

Change password (three-field form), Two-factor authentication (enable/disable TOTP), Reset two-factor authentication (via support), End all sessions.

4.7 Verification (KYC)

The verification screen surfaces the current verification status (pending verification, in review, verified, rejected), a summary of documents already submitted, a control to upload new or replacement documents through the integrated identity-verification provider's in-page interface (see §3.3), and where verification is rejected, a message indicating the reason and a button to re-submit.

4.8 Sessions

A table of recent login sessions with Session ID, Device/browser, Source IP, Started at, Last activity at. The screen offers "End this session" and "End all other sessions" buttons.

4.9 Finance — financial transactions history

A history of the player's deposits and withdrawals: Transaction ID, Type, Method, Amount, Currency, Status, External reference, Created at. Filtering by type, status, and date range.

4.10 Game transactions

Detailed history of every casino game round the player has played, with bet amount, win amount, balance before/after, game name, provider, and timestamp.

4.11 Sport history

Detailed history of every sports coupon the player has placed: coupon ID, stake, potential return, status (open, settled, cashout, void), legs (event, market, odds, leg status), and placement timestamp.

4.12 Bonus history

History of bonus assignments — awarded, accepted, declined, active, redeemed, expired, or rejected.

4.13 Free-spin history

History of free-spin grants: game name, provider, granted count, used count, status, validity end date.

4.14 VIP

The player's view of their VIP tier: current tier name, progress to the next tier, tier-specific benefits, a link to the public VIP description.

4.15 Account limitation

Self-service responsible-gambling limits.

Limit type	What it caps	Period
Deposit limit	Maximum amount the player may deposit	Daily, weekly, monthly
Loss limit	Maximum cumulative loss before play is blocked	Daily, weekly, monthly
Wager limit	Maximum amount the player may wager	Daily, weekly, monthly
Session limit	Maximum length of a single session before automatic sign-out	In minutes

4.15.1 Account-level financial rules

In line with the Account Management Policy:

- **Funds reflection.** Deposited amounts are credited to the player's wallet immediately upon completion of the bank's standard processing procedure.
- **Withdrawal — cash.** For cash settlement the player must present an identity document — passport, national ID card, or driving licence.
- **Withdrawal — cashless.** Cashless settlement is performed to the player's nominated bank account.
- **Loss debit.** Losses are deducted from the wallet immediately upon settlement of the round.
- **Insufficient balance.** A player whose balance is insufficient to place a wager cannot play.
- **Play on credit is prohibited.**
- **Withdrawal during suspension.** Withdrawals cannot be performed while the account is suspended.
- **Misuse of the account.** Where the player misuses the account dishonestly, a fine is imposed.

4.16 Cooling-off period

A short responsible-gambling pause. The player chooses a duration (e.g. 24 hours, 7 days, 30 days). During the cooling-off period the player cannot deposit or wager; they retain read-only access to their account history. The

cooling-off cannot be cancelled before its end date.

4.17 Self-exclusion

A longer, more decisive responsible-gambling control. The player chooses a self-exclusion period (typically 6 months, 1 year, 5 years, indefinite). During the period the player cannot sign in, any remaining balance is paid out, marketing communications stop, and re-registration attempts at the same identity are blocked.

4.18 Notifications

Within the dashboard, a notifications surface shows messages from the operator: welcome messages, bonus offers, KYC reminders, withdrawal status updates, responsible-gambling reminders.

4.19 Activity log (the player's own history)

The player's view of their own actions: sign-ins, password changes, profile edits, deposit / withdrawal events, bet / win events.

4.20 Account closure (player-initiated)

The Account Management Policy provides that the player may request closure of their account at any time. Account closure is handled out-of-band — through a support channel — so that identity can be re-confirmed.

Procedure:

1. The player contacts the operator by phone, live chat, or email (support@portobahis684.com).
2. The player is asked to confirm their identity (see §4.22).
3. After successful re-identification, the account is closed.
4. A confirmation is sent to the player's registered contact channel.

4.21 Self-blocking (player-initiated)

The Account Blocking Policy provides a structured self-blocking procedure as a stronger control than account closure.

Procedure:

1. The player sends an email to support@portobahis684.com .
2. The email must include a photograph of the player's identity document, a selfie holding the identity document, and a signed written request for blocking.
3. The operator reviews the request within 48 hours.
4. On approval, the account is blocked.

4.22 Identification procedure for support requests

Whenever the player makes a sensitive request, the operator confirms identity before acting. The standard identification set is: Personal identification number, First name and surname, Date of birth, Username or the email registered to the account.

4.23 Phone-number change

The player contacts the operator via chat, email, or messenger and sends photographs of the identity document, a selfie holding the document, and the new phone number. The account manager sends an SMS code to the new number for confirmation.

4.24 Email-address change

The player sends photographs of the identity document and a selfie holding the document, together with the new email address. Verified email: full procedure applies. Unverified email: full identification is sufficient.

4.25 Transaction statement request

A player may obtain a formal statement of their deposits and withdrawals for a chosen period. The operator sends the player a transaction-statement application form; the player completes it and sends it to

support@portobahis684.com, attaching photographs of the identity document and a selfie. The response is sent within ten working days.

4.26 Certificate of blocked-account status and certificate of non-existence of account

The Account Blocking Policy provides for two formal certificates the player may request. Both follow the same procedure as the transaction-statement request (§4.25).

4.27 Dormant account policy

- An account is considered dormant if it has not been used for one year.
- Dormant accounts are closed by the operator.
- Funds held in a dormant account are considered "abandoned" from the moment dormancy is recognised.
- At least 60 days before treating funds as abandoned, the operator must take reasonable steps to locate the player.
- Abandoned funds are placed in a dedicated account and, on request, the operator notifies the competent authority.
- Resuming activity — the player can suspend the dormancy process at any time simply by signing in or completing a transaction.

4.28 Special-situation procedures

Situation	Operator handling
Account blocked by the Revenue Service while a balance is held	The player contacts the operator via email and provides identity-document photographs, a selfie with the document, the bank account number to which the balance should be transferred, and the recipient's full name.
Deceased customer with a balance	The family contacts the operator and provides death certificate, certificate of inheritance, identity-document photographs of the heir, a selfie of the heir with their document, and the heir's bank account for transfer.
Self-harm threat from the player	The operator offers the standard self-blocking procedure. Exception: if the player presents an immediate threat with an urgent request to block, the operator blocks the account immediately and records a note.

Chat-based misconduct	Players are prohibited from sending illegal, profane, immoral, threatening, or advertising messages in any chat; the operator reserves the right to disconnect a player who breaches this rule.
-----------------------	---

5. Game Categories and Search

This section describes how the game catalogue is organised on the website, how players browse and filter games, and how the search affordance works.

5.1 Catalogue scope

The website's catalogue covers the full range of products integrated by the operator:

Product	Surfaces	Game types
Casino — slots	<code>/slots</code> , <code>/browse-slots</code> , <code>/games</code>	Video slots, classic slots, jackpot slots, hold-and-spin titles, megaways, branded slots
Casino — live	<code>/live-casino</code> , <code>/browse-live</code>	Live roulette, blackjack, baccarat, game shows
Casino — table	within <code>/slots</code> and <code>/games</code>	Roulette (RNG), blackjack (RNG), baccarat (RNG)
Casino — virtual	within <code>/slots</code> and <code>/games</code>	Virtual sports, virtual races, instant-result games
Casino — crash / instant	within <code>/slots</code> and <code>/games</code>	Crash games, mines, plinko, and similar instant titles
Sportsbook (pre-match)	<code>/sportsbook</code>	Football, basketball, tennis, ice hockey, baseball, MMA, motorsport, etc.
Sportsbook (live)	<code>/live-sport</code>	Same sport range, in-play
Esports	<code>/esport</code>	CS, DOTA, LoL, Valorant, and similar competitive titles

5.2 Game categorisation

Standard categories include: Featured, Popular / Top games, New, Slots, Live casino, Table games, Jackpots, Megaways, Crash & instant, Virtual sports, Bonus buy, Themed categories.

5.3 Lobby layout

The casino lobby is composed of top filter row (active category tabs), provider strip (logos of providers), curated rows ("Featured", "Popular", "New"), main grid, game tile, and sort selector.

5.4 Filtering

Each lobby supports filtering by Category, Provider, Bet limit, Volatility, RTP, Bonus features, Dealer language, and Favourites. Filters combine with logical AND.

5.5 Search

The search affordance is reachable from a search icon in the top header on every page. Results appear within a few hundred milliseconds. The search index covers game title, provider name, category name, and tags/themes.

5.6 Game tile and launch

A game tile is a clickable card with the game cover image, title, provider name (smaller text), small overlay badges, a favourite toggle for authenticated players, and a play/demo affordance.

5.7 Provider directory

The provider directory at `/providers` lists every integrated content provider as a clickable logo grid.

5.8 Favourites

Authenticated players can mark any game as a favourite. Favourites synchronise across devices.

5.9 Sportsbook structure

The sportsbook offers sport navigation, time-based slices, featured events, betslip, and "my bets" showing live and recently-settled coupons.

5.10 Live-sport structure

The live-sport surface is similar to the sportsbook but limited to events currently in play. Markets update in real time.

5.11 Esports structure

The esports surface is provided through an integrated esports provider. It mirrors the sportsbook structure with esports-specific competitions and markets.

5.12 Catalogue freshness

The catalogue is kept fresh through the operator's content team managing games in the admin back-office; changes are visible on the website shortly after publication.

5.13 Demo mode

Where the upstream provider supports demo mode, unauthenticated visitors can launch a game in demo mode from the game tile.

5.14 Accessibility and discovery

Game tile alt-text and provider labels are translated. Keyboard navigation is supported in the search overlay (arrow keys, Enter).

6. Promotions and VIP Program

This section describes the marketing and loyalty surfaces of the website — how promotions are presented, claimed, and tracked, and how the VIP programme is structured.

6.1 Promotions overview

The website carries an active promotions programme. Promotions are short-lived marketing offers defined by the operator's marketing team.

6.1.1 Where promotions appear

Home page (hero slider), Promotions index (`/promotions`), Promotion detail (`/promotions/:slug`), Popups, Notifications, Email and SMS.

6.1.2 Promotion contents

Each promotion exposes: Image/banner, Title, Body, Terms & conditions, Start and end dates, Eligible customer groups, Call-to-action.

6.2 Promotion lifecycle

Stage	Player view
Active	Promotion appears in the promotions index
Eligible to claim	A "Claim" or "Opt in" call-to-action is presented
Claimed	The player has opted in; the bonus appears in their bonus history
Wagering	The player sees a wagering counter that decreases as qualifying bets are placed
Redeemed	Wagering met; the bonus converts to real balance
Expired	The validity window elapsed without meeting the wagering requirement
Closed	The promotion's overall validity window has ended

6.3 Bonus mechanics

The operator's bonus catalogue supports Deposit-match, Fixed-amount bonus, Free spins, Cashback, Tournament prize, No-deposit bonus, and Re-deposit bonus. Each bonus carries parameters: Value, Minimum deposit, Maximum amount, Wagering requirement, Validity window, Eligible games, Eligible customer groups, Geographic eligibility.

6.4 Cashier surfaces for bonuses

Within the cashier, the player sees available bonus offers attached to a deposit, the opportunity to opt in or out, and a note about the wagering requirement.

6.5 Bonus history

The Bonus History screen in the profile (§4.12) is the player's authoritative view of every bonus ever offered, claimed, or redeemed.

6.6 Free spins

The Free-Spin History screen (§4.13) lists every free-spin grant the player has received.

6.7 Cashback

Cashback (a refund of a percentage of net casino losses) is presented as a recurring benefit whose value depends on the player's loyalty tier and on the period.

6.8 Tournaments and "Drops & Wins"-style promotions

Provider-driven promotions such as "Drops & Wins" (Pragmatic Play), provider tournaments, and operator-defined tournaments are surfaced through their own promotion entries.

6.9 Marketing channels

For players who have opted in: Email, SMS, In-app notifications, Browser push (where supported). Opt-in is collected at registration and can be changed from the Settings screen.

6.10 VIP Program — overview

The VIP programme rewards loyalty with a tier-based set of benefits.

6.10.1 Tiers

Tier	Position
Bronze	Entry tier; default for new verified players
Silver	First progression
Gold	Mid-tier
Platinum	Senior tier
Diamond	Top tier

6.10.2 Tier benefits

Benefits scale with tier and include Cashback percentage, Personal VIP host, Withdrawal priority, Higher transaction limits, Birthday bonus, Exclusive promotions, Custom gifts / invitations.

6.10.3 Where the VIP programme is surfaced

Public VIP page (/vip), Profile VIP screen (/account/vip), Profile header, Promotions index, Notifications.

6.10.4 Tier transitions

The platform supports both upgrades and downgrades.

6.10.5 VIP host

For Gold-tier and above, a dedicated VIP host is assigned to the player.

6.11 Anti-abuse controls

Promotions are subject to anti-abuse controls: One-claim-per-account enforcement, Geographic eligibility, Customer-group eligibility, Wagering-game restrictions, Maximum bet during wagering, Multi-account detection.

7. Customer Support (Support Services)

This section describes the support channels available to visitors and players, the topics each channel handles, and the way support interactions are surfaced on the website. The basis for the channels and timing commitments below is the operator's Disputes and Complaints Policy, Account Blocking Policy, and Account Management Policy.

7.1 Support channels

Channel	Where it appears	Audience	Operating hours / SLA
Live chat	Floating launcher button on every page (bottom-right)	Visitors and authenticated players	24 hours / 7 days
Operational email — support@portobahis684.com	Listed in the footer and on the Contact page	Visitors and players	Routine: same business day. Transaction statements / certificates: within 10 working days. Self-blocking requests: within 48 hours.
Complaints / disputes email — support@portobahis684.com	Listed in the footer and on the Contact page	Visitors and players	Formal claims reviewed within 30 calendar days of submission.
VIP host (direct)	Reachable from the VIP-tier screens (Gold and above)	Eligible VIP players	Per the host's published availability
Help / FAQ pages	Linked from the footer	Visitors and players	Always available
In-app notifications	Notifications drawer in the profile	Authenticated players	Real-time delivery

7.2 Live chat — overview

The live chat is the primary, real-time channel for player support.

7.2.1 Launcher

A floating chat launcher appears on every screen at the bottom-right of the viewport with a chat-bubble icon, a red badge indicating unread messages, and a short hover tooltip for desktop users.

7.2.2 Chat window

Opening the launcher reveals the chat window with Header (brand name, agent name, close button), Message area, Composer (text input with send button, attachment button, and emoji selector), and Pre-chat form (for first-time visitors).

7.2.3 Authenticated player context

When an authenticated player opens the chat, the support team automatically receives the player's basic context (account name, account state, VIP tier, current balance, last successful sign-in, source IP and device). Sensitive context (document images, passwords) is not included.

7.2.4 What the chat handles

General product questions, account questions, bonus and promotion questions, responsible-gambling support, sign-in/password-recovery assistance, technical-issue triage, initial intake of account-management requests, escalation to a senior agent or the VIP host.

7.2.5 What the chat does not do

- It does not initiate transactions (deposits or withdrawals) on behalf of the player.
- It does not accept credentials from the player.
- It does not reveal another player's data.
- It does not override responsible-gambling controls.
- It does not carry out account-management actions without the documented evidence sent to the operational email address (support@portobahis684.com).

7.2.6 Localisation

The chat window inherits the player's currently-selected language.

7.2.7 Persistence

For authenticated players, conversations persist across sessions.

7.2.8 Operator-side surfaces

On the operator side, the support team uses the integrated support-service back-office.

7.3 Support email

Email	Purpose
support@portobahis684.com	Operational matters — account-management requests, transaction-statement and certificate requests, document submission, technical assistance, KYC follow-up, formal complaints and disputes.

Out-of-band procedures handled by email include Self-blocking (within 48 hours), Transaction statement request (10 working days), Certificate of blocked account (10 working days), Phone-number change, Email-address change, Blocked-account balance handling, Deceased customer balance handling.

7.4 Integrated support service

The live-chat surface on the website is provided through an integrated third-party support service. The integration carries the player's authenticated context, stores conversation transcripts, does not store credentials or KYC documents, and operates over HTTPS.

7.5 Help, FAQ, and informational pages

Page	Content
About us	Operator identity, brand story, history
Contact	Support channels, email address <code>support@portobahis684.com</code> , operating hours
Help / FAQ	Frequently asked questions
Rules (General Provisions / Terms and Conditions)	The platform's full Rules
Personal Information Management	The operator's privacy and personal-data policy
Data Protection	The operator's data-protection statement
Cookie Policy	Cookie usage and the cookie-consent dialog
Responsible Gambling	The operator's responsible-gambling policy
AML Policy	The operator's anti-money-laundering posture
Self-Exclusion	A standalone explanation of self-exclusion options
Game Rules	Pointer to provider-specific game-rules pages
Sport Rules	Pointer to sportsbook rules
Withdrawal Policy	Description of withdrawal limits, processing times, verification requirements

7.6 Notifications (in-app)

Notifications surfaced in the dashboard are a second support / communication channel: Welcome, KYC reminders, Withdrawal status, Bonus offers, Bonus status, Responsible-gambling reminders, Security events, Promotion announcements, VIP transitions, Dormancy warning.

7.7 Complaints and dispute handling

7.7.1 How to file a complaint

Any written complaint or claim may be filed via email at `support@portobahis684.com`.

7.7.2 Response timeline

The operator's administration reviews each complaint within 30 calendar days of submission. The decision is communicated to the player in the same form in which the complaint was lodged.

7.7.3 Evidentiary basis

Information on every wager placed on the platform is stored in the Portobahis database maintained by შპს „პორტობაჰის ინვესტიმენტი“. In any disputed situation, the electronic record stored in the platform's archive is decisive. Information on a placed wager is retained at least until the corresponding winnings have been paid out.

7.7.4 Holding the balance during dispute

In the event of a disputed situation, the operator reserves the right to hold the player's balance until the situation is resolved.

7.7.5 Force-majeure

In the event of force-majeure circumstances, the operator is relieved of any obligations during the duration of the event.

7.7.6 Escalation

If the player is not satisfied with the operator's response, the player may escalate through the procedures available under the applicable Georgian gambling legislation and through the Revenue Service's dispute-resolution channels.

7.8 VIP host (direct support)

For Gold-tier players and above, a dedicated VIP host is assigned. The host is reachable through a direct line from the live-chat window and a direct email address provided to eligible players.

7.9 Operating hours and response times

Channel	Availability	Response-time target
Live chat	24 hours / 7 days	Live agent during open hours
support@portobahis684.com	24/7 inbound	Routine: same business day. Self-blocking: within 48 hours. Statements / certificates: within 10 working days. Formal claims: within 30 calendar days.
VIP host (direct)	Per host availability	Per host commitment

7.10 Accessibility

The chat is keyboard-navigable, supports screen-readers, and text is resizable through the browser's standard zoom. Colour contrast meets standard accessibility levels.

8. Language and Localisation

This section describes the website's supported languages, where the language switcher appears, how the player's choice is applied across surfaces, and how localised content is administered.

8.1 Supported languages

The website is delivered in two interface languages for the Georgian property at <https://portobahis684.com/>:

Code	Language	Status
ka	Georgian	Default interface language
en	English	Alternative interface language

The platform opens in Georgian by default. The player can switch to English at any time from the language switcher in the top header; the choice is persisted across visits.

8.2 Language switcher — where it lives

The language switcher appears in the top header on every page and is visible to both unauthenticated visitors and authenticated players. On mobile the switcher is exposed inside the collapsed (hamburger) menu. The switcher button shows the current language.

8.3 Language selection — behaviour

Aspect	Behaviour
Initial language	Georgian on first visit.
Persistence	The selected language is persisted client-side and restored on subsequent visits from the same browser.
Authenticated players	The selection is also recorded server-side against the player's account.
Change effect	Switching language re-renders the website immediately — no page reload required.
Marketing and notifications	Notifications and marketing emails / SMS are sent in the player's selected language.

8.4 Where the language is applied

Both Georgian and English are applied uniformly across the platform: Top navigation labels, Page titles/headings/body copy, Buttons/links/CTAs, Form labels/placeholders/validation messages, Error messages, Notification messages, Footer copy/legal links, Hero slider creatives, Promotion titles/body/terms, Static pages, Email and SMS templates, Integrated identity-verification interface, Integrated live-chat surface.

8.5 What is not translated by the website

Some surfaces are owned by third-party providers and follow that provider's own localisation:

Surface	Localisation source
Sportsbook content (event names, market names)	Provided by the upstream sportsbook engine
Live-sport in-play markets	Same
Esport event names, market names	Provided by the integrated esports provider
Casino game content (in-game text)	Provided by each casino game provider
Provider names and logos	As supplied by the provider

8.6 Numeric and date formatting

Format	Georgian (ka)	English (en)
Thousands separator	Space or comma	Comma
Decimal separator	Comma	Dot
Currency display	Symbol alongside the amount	Symbol alongside the amount
Date format	DD-MM-YYYY	DD-MM-YYYY (24-hour, per operator policy)
Time format	24-hour	24-hour

8.7 Translation management

Translation strings are administered through the admin back-office translation editor. A system administrator can edit any translation key, add missing entries when a new feature is rolled out, and update copy in response to localisation feedback without requiring a redeployment of the website.

8.8 Quality assurance

- Every translation key has a fallback value to prevent a broken display.
- Translation keys that are missing in the player's chosen language render their fallback rather than the raw key.
- The translation editor surfaces missing-translation gaps to the content team for prioritisation.

8.9 Accessibility considerations

Aspect	Behaviour
HTML lang attribute	The page's <code><html lang></code> attribute is set to <code>ka</code> or <code>en</code> according to the player's current language.
Font choice	The chosen typeface supports the Georgian script (Mkhedruli alphabet) and the Latin alphabet in full.
Character rendering	Unicode-aware throughout; both scripts render correctly across all browsers and devices.

Text resizing	Standard browser zoom respected.
Colour contrast	Meets the operator's accessibility level.

9. Security and Data Protection

This section describes the security and data-protection controls applied to the website itself — the player-facing surfaces, the data the website handles, and the boundaries between the website and external systems. The control set described here is grounded in the operator's published policies:

- Personal Information Management Policy
- Data Protection Policy
- Network Security Policy
- Anti-Fraud Security Policy
- AML Policy (Official, approved 24 January 2026)

9.1 Transport security

All traffic between the player's browser and the website is carried over HTTPS (TLS). The platform is reachable only on `https://portobahis684.com/` ; HTTP requests are redirected to HTTPS at the edge. TLS termination is performed at the edge (Cloudflare).

Control	Mechanism
TLS termination	Cloudflare edge
Certificate management	Cloudflare-managed
HSTS	Enabled
Mixed-content	Not permitted; all referenced assets load over HTTPS
Cipher suite policy	Edge-managed; TLS 1.2 minimum, aligned with current industry baselines

9.2 Bot protection

Two complementary bot-protection mechanisms operate on the website: Cloudflare WAF + Turnstile (edge-level filtering), and an invisible anti-bot challenge at the login, registration, and forgot-password forms.

9.3 Authentication

9.3.1 Credentials

- The player chooses a username and a password at registration.
- Password complexity is enforced server-side.
- Passwords are stored as cryptographic hashes server-side.
- Passwords are never displayed back to the player.
- Sharing of credentials with third parties is prohibited.

9.3.2 Failed-login protection

Control	Behaviour
Rate-limiting	Repeated failures from the same source are slowed and ultimately rejected by the edge / back end.
Account lockout — three failed attempts	After three (3) consecutive unsuccessful sign-in attempts the account is automatically locked. The player must initiate the password-recovery flow (§3.5) or contact support (§7) to restore access.
Generic error messages	Failures return the same translated message whether or not the account exists.
Suspicious-location alerts	A sign-in from a new device or location triggers a notification.

9.3.3 Two-factor authentication

The website supports time-based one-time password (TOTP) two-factor authentication using any standard authenticator application. Standard TOTP (RFC 6238) with a 30-second rotation interval.

9.3.4 SMS phone verification

SMS phone verification is required on registration.

9.3.5 Session management

Session token issued by the back end on successful sign-in; bound to the browser; carried over HTTPS only. Sessions expire after a server-defined inactivity window. "Remember me" extends the session lifetime.

9.4 Authorisation and access control

Every request from the website to the back end carries the session token; the back end identifies the requesting player, checks whether the action is permitted, and ensures data scoping (a player cannot read another player's data).

9.5 Operator-side governance and security organization

In line with the Network Security Policy the operator maintains a defined security-governance structure:

Role	Responsibility
Management Board	Approves the security policy and provides system-wide oversight.
CISO (Chief Information Security Officer)	Accountable for IT security across the operator.
Compliance / AML Officer	Accountable for KYC and AML monitoring and reporting.
AML Unit	The executive unit that implements the AML policy and CDD procedures (see §9.8).
IT Teams	Accountable for systems integration and operational monitoring.
All staff	Required to follow the security policy and to take part in periodic training and security checks.

9.6 Data security

9.6.1 Encryption

Player data is stored in encrypted format; AES-256 (or stronger) encryption algorithms are used; records are kept on three protected servers (production, development, backup).

9.6.2 Access management for operator staff

Multi-factor authentication (MFA) mandatory for operator staff sign-in. Role-based access control (RBAC). Administrative accounts limited to a defined set of authorised individuals.

9.6.3 System and network security

Next-generation firewall at the network perimeter, IDS/IPS on every input/output interface, penetration/regression testing at least every 30 days, centralized SIEM log monitoring with daily analysis, encrypted VPN with MFA for remote access.

9.6.4 Software lifecycle

Each service and software component receives updates on a defined release cycle. Critical patches distributed within 24 to 72 hours of issue. Static and dynamic security testing on all code.

9.6.5 Real-time transaction monitoring

All operations recorded in real time and feed into SIEM and AML systems. Behavioural analytics and risk-scoring algorithms applied. Atypical transactions flagged automatically to the Compliance Officer.

9.7 Personally identifiable information (PII)

9.7.1 Categories of PII

Category	Examples
Identity	First name, surname, father's name, date of birth, place of birth, citizenship, country of residence, personal identification number
Contact	Email address, mobile phone, residence address
Documents	Identity-document images and live-selfie biometric data captured during the Liveness Check
Account	Username, password (hashed), wallet currency, account status
Activity	Sign-in IP and user-agent, session history, game-round history, bet history, deposit/withdrawal history, bonus history
Preferences	Language, marketing consents, responsible-gambling limits

9.7.2 Lawful basis and PII handling principles

- Processing is based on the player's express consent at registration.
- Data is processed fairly and lawfully, without prejudicing the data subject's dignity.
- Data is processed only to the extent necessary to achieve the lawful purpose.

- Data must be accurate, true, and updated where necessary.
- Data may be retained only for the time required to achieve the purpose of processing.
- Personal data is not shared with third parties, except: legally mandated exceptions, persons providing services on the operator's behalf, and partners required for service improvement and provision.
- Each member of the operator's personnel is bound to confidentiality.

9.7.3 Direct-marketing data

For direct-marketing purposes the following categories may be processed where the player has consented: Name, Address, Telephone number, Email address. The player may at any time request that the operator cease processing personal data for direct-marketing purposes; the operator stops within ten working days.

9.7.4 Data subject rights

The player may at any time request the personal data the operator holds about them, withdraw the consent given at registration, or switch off marketing communications.

9.7.5 KYC documents and biometric data

Identity documents and biometric data are submitted through the integrated identity-verification provider's in-page interface (see §3.3). Biometric data is protected by all reasonable technical and organisational means; retention is limited to the period required by law.

9.7.6 Payment data

Payment-instrument data (card numbers, account numbers, cryptocurrency addresses) is handled by the integrated payment-service providers, not by the website itself. This is the standard practice for compliance with PCI-DSS scoping.

9.7.7 Marketing consent

Marketing consent is captured at registration and can be modified at any time from the Settings screen.

9.7.8 Third-party analytics

The operator may use third-party services including Hotjar to better analyse user behaviour and interaction with the website. Data is used only for the purpose of improving website functionality.

9.8 Anti-Money-Laundering (AML) and Counter-Terrorism Financing

The operator maintains an official AML policy approved on 24 January 2026 at Batumi, Georgia. The policy is based on:

- The Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism.
- The Third Anti-Money-Laundering Directive of the European Union (26 October 2005).
- Government of Georgia decree №2257 of 30 October 2019 on the National Risk Assessment Report and Action Plan.
- FATF recommendations.

9.8.1 AML governance

The operator's AML sub-unit is the executive organ that implements AML procedures. Every staff member is required to exercise due care and to escalate any suspicious signs.

9.8.2 Customer Due Diligence (CDD)

The operator applies a standard CDD method to every client who registers on the platform (see §3.3.4).

9.8.3 Reporting thresholds

Preventive measures must be applied where:

- A cash inflow, a payout, or the aggregate of related transactions exceeds GEL 5,000 (or the equivalent in another currency).
- A business relationship is established for the purpose of organising lotteries, gambling, or other prize games in electronic-system form.

9.8.4 Risk classification

Standard risk levels: Low (every five years re-identification) and High (every year, includes PEPs and suspicious activity clients).

9.8.5 Grounds for terminating the client relationship

The operator has the right to refuse or terminate the business relationship for breach of agreement, non-gambling use of accounts, third-party access, relationship with a shell bank, reasonable suspicion of money laundering or fraud, or any client on a list of terrorists.

9.8.6 Reporting and record-keeping

The operator submits reports on suspicious transactions (and attempts) to the Ministry of Finance.

- On request, the operator provides the Ministry of Finance (or other authorised state body) with any information obtained under the law about a transaction or transaction participant.
- Reporting is filed on the same day as reasonable suspicion arises.

The operator retains all information obtained under the AML Law, the analyses performed, the client account documentation, and the business correspondence for five years from the end of the business relationship or single transaction. Records are retained for five years from the end of the business relationship, in a form that allows submission to the competent body.

9.8.7 Confidentiality of AML information

The operator and its staff are prohibited from informing the client or any third party that an unusual or suspicious transaction is under study.

9.9 Anti-fraud framework

The operator maintains a dedicated Anti-Fraud Security Policy covering both internal and external fraud risk.

Highlights: Strengthened internal controls, all staff required to participate in fraud prevention, risk-management/internal-security function, culture of integrity through staff training.

9.10 Cookies and local storage

Purpose	Storage
Session token	Cookie (HttpOnly where the browser allows)
Language preference	Local storage
Theme preference	Local storage
Cookie-consent state	Local storage
Anti-bot challenge state	Provider-managed cookie
Analytics (Hotjar and equivalents)	Provider-managed cookie, only where the player has consented

9.11 Realtime channel

A realtime push channel (WebSocket-based) is used for the live online-player count, live updates of "live winners" tiles, in-app notifications, and live counters in the cashier and game frames. The realtime channel carries no PII.

9.12 Third-party integrations and data flows

Integration	Data flows
Edge / WAF (Cloudflare)	All HTTPS traffic transits Cloudflare; Cloudflare sees request metadata but no payload-side credentials.
Identity-verification provider	KYC documents and biometric data are collected through the provider's in-page interface.
Payment-service providers	At deposit or withdrawal, the player is moved into the PSP's tokenised flow.
Sportsbook providers	Coupons placed by the player and the resulting market state are exchanged with the upstream sportsbook engine.
Casino game providers	Game-round events are exchanged with the upstream provider through the embedded game frame.
Realtime channel provider	Non-sensitive realtime messages.
Live-chat / support service	Conversation transcripts and the player's authenticated context.
Hotjar (or equivalent analytics)	Aggregate behavioural metrics, used only to improve website functionality and user experience.

9.13 Communications monitoring

In line with the Personal Information Management Policy, the operator has access to call recordings and other communication channels (email, messaging, chat) and conducts monitoring for dispute resolution and prevention of dishonest or unlawful conduct.

9.14 Incident response

The operator maintains an incident-response procedure. Security incidents trigger an automated notification to the SIEM and Compliance systems. Response steps: incident categorisation, isolation, root-cause analysis, effective

remediation, documentation.

9.15 Compliance and audit

The Network Security Policy aligns with the Georgian legislation governing online gambling and personal-data protection, European Union regulations including the GDPR baseline, PCI DSS for payment-card-related scope, and ISO 27001 as the information-security management baseline. The operator undergoes annual independent external audits.

9.16 Staff training

Operator staff complete security training on a monthly cadence, covering the Security Operations Centre (SOC) and phishing-analysis standard programmes.

9.17 Out of scope

The following security topics are out of scope for this document and are addressed in the operator's broader security and compliance documentation: Server-side cryptography key management, Database-level access control specifics, Internal network topology, Disaster-recovery drills, Cloud-provider security posture, Source-code-management security.

10. Platform Technical Specifications

This section consolidates the technical-platform specifications that complement the operational and compliance descriptions in sections 1–9. The content is provided by the operator's engineering team and corresponds to the operator's Platform Technical policies.

10.1 System architecture and network topology

Overview

The platform utilises a high-availability, hybrid-cloud architecture primarily hosted on AWS (Amazon Web Services), with a secondary redundant infrastructure hosted on Voxility for real-time replicas and off-site backups.

Network isolation

All application components — Backend, Database, and Cache — are isolated within a Private Subnet / VPC. They are configured to accept only local connections from the authorised API Gateway / Load Balancer. Public access is strictly prohibited at the instance level.

Seamless wallet integration

The integration between the Game Engine and the Wallet Provider is handled via a secure REST API protocol. Every transaction follows a strict handshake and verification process before the balance is updated.

Central topology

The system is divided into: Frontend Layer (2 dedicated nodes), Backend API Layer (2 dedicated nodes), High-availability Database Cluster managed via HAProxy.

Architecture summary

Aspect	Specification
Primary cloud	AWS (Amazon Web Services)
Secondary cloud	Voxility — real-time replicas and off-site backups
Network model	Private Subnet / VPC — public access strictly prohibited at instance level
Frontend layer	2 dedicated nodes
Backend API layer	2 dedicated nodes
Database	High-availability cluster managed via HAProxy
Integration protocol	Secure REST API with strict handshake and verification
Public access	Only via authorised API Gateway / Load Balancer

10.2 Hardware and software inventory

Category	Specification
Operating System	Ubuntu 24.04.4 LTS (Noble Numbat)
Web Server	Nginx 1.27
Runtime Environments	PHP 8.5, Go 1.24, Node.js v22
Database (RDBMS)	PostgreSQL 16
Caching / NoSQL	Redis 7.0
Monitoring & Logging	NetData, Prometheus, Grafana
Instance Distribution	2× Backend Nodes, 2× Frontend Nodes
Database Nodes	1× Master, 1× Read-Only, 1× Replica (via HAProxy)

10.3 "Malfunction Voids All Pays" notice

Implementation statement. To comply with regulatory standards, the mandatory notice "Malfunction Voids All Pays and Plays" is permanently displayed within the Global Footer of the platform. This ensures the notice remains visible to the user at all times, regardless of the specific game or page they are currently accessing.

10.4 Data retention policy (three-year minimum)

Storage strategy

The system is configured to retain all transaction logs, malfunction data, and game history for a minimum of three (3) years in production; older data is migrated to long-term archival storage where it remains accessible indefinitely.

- **Primary Storage.** Active logs are stored within the AWS ecosystem.
- **Archival.** Older data is migrated to long-term storage solutions (leveraging AWS and Voxility's infrastructure) to ensure durability and availability for audit purposes.
- **Multi-provider durability.** This multi-provider approach ensures that logs remain accessible even in the event of a provider-specific service interruption.

10.5 Disaster Recovery and Business Continuity Plan (BCP)

Automated provisioning and Infrastructure as Code (IaC)

The platform utilises a Declarative Infrastructure model to ensure rapid recovery and environment consistency.

- **Infrastructure as Code (IaC).** The entire production environment — including VPCs, Security Groups, and Load Balancer configurations — is defined as code.
- **Automated configuration management.** Automated orchestration provisions the Ubuntu 24.04 environment with hardened security patches, runtime versions, and service configurations.
- **Immutable infrastructure.** Servers are treated as immutable to prevent configuration drift.
- **Rapid restoration (RTO).** The Recovery Time Objective (RTO) is capped at 10–30 minutes.

Data redundancy and failover logic

- **High-availability (HA) database cluster.** Using a Master-Replica architecture behind HAProxy.
- **Cross-cloud synchronisation.** A real-time data bridge is maintained between AWS and Voxility, ensuring a Recovery Point Objective (RPO) of near-zero.
- **Validation.** Recovery procedures are tested quarterly to ensure the automated provisioning logic remains synchronised with the current production baseline.

Summary

Aspect	Specification
Recovery Time Objective (RTO)	10 – 30 minutes
Recovery Point Objective (RPO)	Near-zero
Infrastructure model	Declarative (Infrastructure as Code)
Server treatment	Immutable
Failover	Automated, HAProxy-fronted HA database
Synchronisation	Real-time, cross-cloud (AWS ↔ Voxility)
Testing cadence	Quarterly

10.6 Time synchronisation

Protocol

All system clocks across the infrastructure are synchronised using the Network Time Protocol (NTP).

Service provider

The platform utilises the AWS Time Sync Service. This ensures that all transaction timestamps, logs, and game results are recorded with microsecond-level accuracy and are consistent across the entire distributed network.

11. Outcome Determination / RNG

General Principles

The Red Lane gaming platform offers various categories of games, including:

- Online Slot Games
- Table Games
- Live Dealer Games
- Instant Win Games
- Crash Games
- Virtual Sports
- Sportsbook
- Esports Betting

Because these products differ technically, the mechanism used to determine game outcomes varies according to the product type.

Each game category follows its own certified outcome determination methodology while maintaining the same fundamental principles of:

- Fairness
- Randomness (where applicable)
- Independence
- Transparency
- Security
- Regulatory Compliance

Random Number Generator (RNG) Games

All RNG-based casino games offered through the Red Lane platform utilize certified Random Number Generator (RNG) technology supplied by licensed third-party gaming providers.

The RNG is a cryptographically secure software algorithm that continuously generates unpredictable numerical sequences regardless of whether a game is actively being played.

When a player initiates a game event (such as pressing the "Spin" button or dealing cards), the gaming system captures the next available random number generated by the RNG.

That number is immediately translated into a specific game outcome using the predefined mathematical model developed and certified by the game provider.

Neither the player nor Red Lane B.V. can influence, predict, manipulate, or alter the generated outcome.

Characteristics of the RNG

The Random Number Generator implemented by certified game providers possesses the following characteristics:

Independence

Every game event is completely independent of previous outcomes. Previous results do not influence future results.

Randomness

Each number generated by the RNG has an equal statistical probability of selection according to the game's mathematical model.

Unpredictability

Generated values cannot be predicted by:

- Players
- Operators
- Employees
- System administrators
- Third parties

Non-repeatability

The RNG continuously produces random values that do not follow identifiable patterns.

Continuous Operation

The RNG operates continuously, even when no players are actively participating.

Because the generator continuously produces random values, no person can predict which value will be selected at the exact moment a game action occurs.

Game Mathematics

Each casino game contains predefined mathematical parameters established by its certified game developer. These include:

- Probability tables
- Reel mapping
- Card distribution algorithms
- Paytables
- Bonus trigger logic
- Jackpot probabilities
- Return to Player (RTP)

These mathematical models are fixed during certification and cannot be modified by Red Lane B.V.

Return to Player (RTP)

Each game is configured with a certified theoretical Return to Player (RTP) percentage determined by the game developer.

The RTP represents the long-term statistical return expected over millions of game rounds and does not guarantee individual player results.

The Company does not modify RTP settings unless explicitly supported by the certified game provider and permitted under applicable regulatory requirements.

Where multiple RTP configurations exist, only certified and approved versions are deployed.

Live Casino Outcome Determination

Live Casino games are conducted by professional dealers in controlled studio environments operated by licensed Live Casino providers.

Game outcomes are determined by:

- Physical playing cards
- Roulette wheels
- Dice
- Baccarat shoes
- Other physical gaming equipment

The outcome depends entirely upon the actual physical event occurring during gameplay. Red Lane B.V. has no ability to influence or alter live game outcomes. All live games are streamed in real time using encrypted video transmission.

Sportsbook Outcome Determination

Sports betting outcomes are determined exclusively by the official results of sporting events. Settlement occurs only after:

- Official confirmation by recognised sports governing bodies;
- Validation by approved sports data providers;
- Application of the Company's Sportsbook Rules.

No sporting result can be influenced by the Company. If official event results are amended after settlement, adjustments are made only in accordance with the applicable Sports Betting Rules.

Virtual Sports

Virtual Sports utilize certified RNG systems combined with predefined animation engines. The RNG determines:

- Match outcomes
- Goal scoring events
- Race winners
- Competitor positions

Animations merely display the previously generated result and do not determine the outcome.

Crash Games

Crash Games operate using certified provably fair or certified RNG technologies supplied by licensed providers. Before each game round begins:

- A random multiplier is generated;
- The multiplier determines the point at which the round ends;

- Players choose when to cash out before the multiplier crashes.

The crash point is predetermined by the certified game engine before the animation begins.

Instant Win Games

Instant Win Games determine results immediately following player participation. Certified RNG algorithms determine:

- Prize values
- Winning symbols
- Bonus triggers
- Game outcomes

The displayed animation only represents the outcome previously generated by the RNG.

Third-Party Game Providers

Red Lane B.V. offers games supplied exclusively by licensed and reputable gaming providers. Each provider is responsible for:

- RNG implementation
- Game mathematics
- RTP calculations
- Software integrity
- Regulatory certification

The Company performs due diligence before integrating any provider.

Independent Testing and Certification

Before deployment on the platform, RNG-based games undergo independent testing and certification by internationally recognised testing laboratories where required by the provider's licensing framework. Testing generally includes:

- Randomness analysis
- Statistical distribution testing
- RTP verification
- Security testing
- Source code review (where applicable)
- Functional testing

Only certified games are made available to players.

Outcome Integrity

To preserve the integrity of game outcomes, Red Lane B.V. implements controls including:

- Secure encrypted communications;
- Digitally signed game transactions where supported;

- Secure API integrations;
- Real-time monitoring of game performance;
- Continuous fraud detection;
- Access restrictions for administrative users;
- Comprehensive audit logging.

Prohibited Activities

Neither Red Lane B.V. nor any employee, contractor, or third party may:

- Modify RNG outputs;
- Manipulate game results;
- Influence sporting event outcomes;
- Alter certified RTP values without appropriate certification and regulatory approval;
- Interfere with certified gaming software.

Any attempt to manipulate game outcomes constitutes a serious breach of Company policy and may result in disciplinary action, contractual termination, regulatory reporting, and legal proceedings.

Monitoring and Continuous Compliance

The Company continuously monitors gaming operations to ensure:

- Correct operation of integrated gaming software;
- Integrity of game outcomes;
- Stability of provider connections;
- Accuracy of settlement processes;
- Compliance with applicable regulatory requirements.

Technical incidents affecting game integrity are immediately investigated, documented, and, where necessary, reported to the relevant provider and competent regulatory authority.

Regulatory Compliance

Red Lane B.V. ensures that all outcome determination mechanisms comply with:

- The requirements of the Curaçao Gaming Authority (CGA);
- The National Ordinance on Games of Chance (LOK);
- Applicable technical standards established by licensed gaming providers;
- Internal governance, security, and operational policies.

The Company does not generate, manipulate, or alter gaming outcomes. All game results are produced through certified systems or official event results, ensuring that every wager is resolved fairly, transparently, and independently.

12. Random Number Generator (RNG) Implementation Standards

Purpose

The purpose of this section is to define the Random Number Generator ("RNG") implementation standards adopted by Red Lane B.V. to ensure that all RNG-based games offered on the Company's gaming platform operate fairly, securely, transparently, and in accordance with the requirements of the Curaçao Gaming Authority (CGA), applicable legislation, and recognised international technical standards.

Red Lane B.V. offers RNG-based gaming products exclusively through licensed and reputable third-party game providers whose gaming software has been independently tested and certified prior to deployment.

Policy Statement

Red Lane B.V. is committed to ensuring that:

- Every RNG-based game produces random, independent, and unbiased outcomes.
- Players have an equal opportunity to win based solely on the mathematical design of each certified game.
- No employee, administrator, supplier, or third party can influence, predict, manipulate, or alter game outcomes.
- RNG implementation complies with applicable regulatory requirements and recognised industry standards.
- Only certified game software supplied by approved providers is made available on the Company's platform.

Scope

These standards apply to all RNG-based gaming products available on the Red Lane platform, including but not limited to:

- Online slot games;
- Digital roulette;
- Blackjack;
- Baccarat;
- Poker variants;
- Video poker;
- Instant win games;
- Crash games using certified RNG technology;
- Virtual sports and other RNG-driven gaming products.

Live dealer games and sportsbook products are subject to separate outcome determination mechanisms and are therefore outside the scope of these RNG implementation standards.

RNG Architecture

The Company does not develop or operate proprietary RNG engines. All RNG functionality is embedded within the certified gaming software supplied by licensed third-party providers. Each provider is responsible for:

- Designing and implementing the RNG;
- Maintaining the mathematical game model;
- Defining the Return to Player (RTP);
- Certifying the software;
- Ensuring ongoing compliance with applicable regulatory requirements.

Red Lane B.V. integrates these certified games through secure APIs and does not alter or interfere with the underlying RNG logic.

Core RNG Requirements

All RNG implementations integrated by Red Lane B.V. shall demonstrate the following characteristics:

Independence

Each random event is independent of all previous and future events. Previous outcomes do not influence subsequent results.

Statistical Randomness

The distribution of generated values must comply with recognised statistical principles, ensuring that outcomes occur with probabilities consistent with the certified mathematical model.

Unpredictability

Random values must not be predictable by:

- Players;
- Company employees;
- Administrators;
- Service providers;
- External parties.

Uniform Distribution

Generated values shall be distributed evenly over time according to the game's approved probability tables.

Non-repeatability

The RNG must not produce deterministic or predictable sequences that could compromise game fairness.

Continuous Operation

The RNG operates continuously regardless of whether games are actively being played, ensuring that the selected value cannot be anticipated when a player initiates a game.

Security Requirements

To preserve the integrity of RNG operations, Red Lane B.V. requires that integrated gaming providers implement appropriate security controls, including:

- Cryptographically secure RNG algorithms where applicable;
- Protection against unauthorised modification of game software;
- Secure software deployment procedures;
- Integrity verification mechanisms;
- Secure communications between gaming servers and the platform;
- Protection against malware, tampering, and code manipulation.

Any software update affecting RNG functionality must be managed through the provider's formal change management process and, where required, re-certified before deployment.

Game Outcome Generation

For RNG-based games, the sequence of events generally follows this process:

1. The RNG continuously generates random values.
2. A player initiates a game action (e.g., spin, deal, or play).
3. The game engine captures the next available random value.
4. The value is mapped to the game's certified mathematical model.
5. The game engine determines the outcome.
6. The outcome is displayed to the player.
7. The transaction is securely recorded in the gaming system.

Once generated, the outcome cannot be modified or influenced by Red Lane B.V.

13. Testing Procedures Implemented by Gaming Providers

Purpose

The purpose of this section is to describe the testing procedures implemented by the licensed third-party gaming providers integrated with the Red Lane B.V. gaming platform. These procedures are designed to ensure that all gaming software operates fairly, securely, reliably, and in accordance with the technical and regulatory standards required by the Curaçao Gaming Authority (CGA) and other applicable licensing authorities.

Red Lane B.V. only integrates gaming content from reputable and licensed providers that have established software development, testing, certification, and quality assurance frameworks. Prior to deployment on the Company's platform, each game must undergo comprehensive testing to verify its integrity, functionality, security, mathematical accuracy, and compliance with applicable regulatory requirements.

Provider Software Development Lifecycle (SDLC)

All integrated gaming providers are expected to follow a formal Software Development Lifecycle (SDLC) incorporating security, quality assurance, and regulatory compliance throughout the development process. The typical SDLC includes:

- Requirements analysis;
- System and game design;
- Software development;
- Unit testing;
- Integration testing;
- Functional testing;
- Performance testing;
- Security testing;
- User Acceptance Testing (UAT);
- Independent certification;
- Production deployment;
- Ongoing maintenance and monitoring.

No gaming software is deployed to the Red Lane production environment until it has successfully completed the provider's internal testing and any required independent certification.

Functional Testing

Providers perform comprehensive functional testing to verify that all game features operate exactly as designed. Testing generally includes verification of:

- Game launch and loading;
- Game rules;
- Winning combinations;

- Paytable calculations;
- Bonus feature activation;
- Jackpot triggers;
- Free spin functionality;
- Gamble feature logic;
- Progressive jackpot calculations (where applicable);
- Auto-play functionality (where permitted);
- Session interruption recovery;
- Error handling;
- Currency display;
- Language localisation;
- User interface functionality.

Each function is tested individually and as part of the complete game flow to ensure consistent operation.

Random Number Generator (RNG) Validation

For RNG-based games, providers perform extensive testing of the RNG implementation to ensure fairness and statistical integrity. Testing includes:

- Randomness analysis;
- Distribution testing;
- Uniformity testing;
- Entropy validation;
- Sequence independence testing;
- Statistical probability verification;
- Long-cycle simulations;
- Verification that previous outcomes do not influence future outcomes;
- Verification that game outcomes correspond accurately with certified game mathematics.

Where required, these tests are independently verified by accredited testing laboratories.

Mathematical Verification

Gaming providers validate the mathematical model underlying each game to ensure that actual gameplay corresponds with the certified theoretical design. Testing includes verification of:

- Return to Player (RTP);
- House edge;
- Hit frequency;
- Volatility;
- Jackpot probabilities;
- Bonus trigger probabilities;
- Symbol weighting;
- Random event distribution;
- Long-term payout consistency.

Large-scale automated simulations involving millions of game rounds are commonly executed to confirm statistical accuracy.

Security Testing

Providers conduct comprehensive security assessments to protect gaming software against unauthorised access, manipulation, and cyber threats. Security testing typically includes:

- Secure coding reviews;
- Vulnerability assessments;
- Penetration testing;
- API security testing;
- Authentication testing;
- Authorisation testing;
- Session management validation;
- Encryption verification;
- Data transmission security;
- Input validation;
- Protection against SQL injection;
- Cross-site scripting (XSS) testing;
- Cross-site request forgery (CSRF) testing;
- Malware detection;
- Code integrity verification.

Any identified vulnerabilities are remediated before software release.

Performance and Load Testing

Gaming providers test software performance under varying operational conditions to ensure platform stability and scalability. Testing commonly includes:

- Concurrent player simulation;
- High transaction volumes;
- Peak traffic conditions;
- Stress testing;
- Load balancing verification;
- Response time measurement;
- Server resource utilisation;
- Database performance;
- API throughput;
- Network latency evaluation.

Performance benchmarks are established to ensure stable operation during periods of increased player activity.

Compatibility Testing

Games are tested across multiple operating environments to ensure consistent functionality. Compatibility testing generally covers:

- Desktop browsers;
- Mobile browsers;
- Android devices;
- iOS devices;
- Various screen resolutions;
- Different operating systems;
- Browser versions;
- Internet connection speeds.

This testing ensures that players receive a consistent gaming experience regardless of device or platform.

Integration Testing

Prior to deployment, providers and Red Lane B.V. verify that gaming software integrates correctly with the Company's platform. Integration testing includes:

- Secure API communication;
- Authentication processes;
- Wallet integration;
- Player account synchronisation;
- Session management;
- Transaction recording;
- Balance updates;
- Bonus engine integration;
- Responsible Gaming controls;
- Error handling and recovery;
- Reporting functionality.

Successful integration testing ensures accurate communication between the provider's gaming servers and the Red Lane platform.

User Acceptance Testing (UAT)

Before production release, User Acceptance Testing is conducted to confirm that the software performs as expected within the operational environment. Testing verifies:

- Overall game functionality;
- Player experience;
- Navigation;
- Registration of wagers;
- Game completion;
- Settlement of winnings;
- Bonus functionality;
- Responsible Gaming tools;

- Reporting accuracy;
- Operational stability.

Any defects identified during UAT are corrected before deployment.

Regression Testing

Whenever software updates or patches are released, providers perform regression testing to ensure that existing functionality has not been adversely affected. Regression testing verifies that:

- Existing games continue to function correctly;
- Previous defects have not reoccurred;
- New software changes do not introduce unexpected behaviour;
- Financial calculations remain accurate;
- Security controls remain effective.

Change Management Testing

All software releases are managed through documented change management procedures. Prior to deployment, providers verify:

- Software version integrity;
- Release documentation;
- Configuration management;
- Deployment scripts;
- Rollback procedures;
- Operational readiness.

Critical updates may require additional certification depending on regulatory requirements.

Incident and Defect Testing

Where software defects are identified, providers follow formal incident management procedures. This includes:

- Logging defects;
- Risk classification;
- Root cause analysis;
- Corrective development;
- Retesting;
- Regression testing;
- Controlled release;
- Post-release monitoring.

Critical defects affecting game integrity are prioritised and resolved before games remain available to players.

Continuous Monitoring

Following deployment, providers continuously monitor gaming systems for operational performance. Monitoring may include:

- Server availability;
- API connectivity;
- Transaction processing;
- Error rates;
- Player session stability;
- Performance indicators;
- Security events;
- Unusual operational behaviour.

Potential issues are investigated promptly to minimise service disruption.

Documentation and Audit Trails

Providers maintain comprehensive records relating to software testing and quality assurance, including:

- Test plans;
- Test cases;
- Test results;
- Defect logs;
- Corrective actions;
- Release approvals;
- Software version histories;
- Security assessments;
- Certification reports.

Where applicable, such documentation may be made available to Red Lane B.V. or competent regulatory authorities upon request, subject to confidentiality and contractual obligations.

Responsibilities of Red Lane B.V.

While the design, development, and testing of gaming software remain the responsibility of the respective licensed gaming providers, Red Lane B.V. performs appropriate due diligence before integration and monitors the operational performance of integrated games. The Company:

- Integrates only licensed and reputable gaming providers;
- Reviews available certification and compliance documentation;
- Tests platform integrations prior to production deployment;
- Monitors technical performance after implementation;
- Investigates operational incidents affecting gaming services;
- Coordinates with providers to resolve technical issues;
- Maintains records relating to provider integrations and operational monitoring.

14. Third-Party Certification

Purpose

The purpose of this section is to describe the independent certification process applicable to gaming software, Random Number Generator (RNG) systems, and related gaming technologies integrated into the Red Lane B.V. platform.

Red Lane B.V. recognises that independent testing and certification are essential components of maintaining a fair, secure, transparent, and compliant online gaming environment. Independent certification provides assurance that gaming software operates in accordance with recognised technical standards and regulatory requirements and that game outcomes are generated fairly and without manipulation.

The Company therefore integrates gaming content only from reputable and appropriately licensed gaming providers that maintain certification of their gaming systems where required under their applicable licensing framework.

Independent Testing Laboratories

Gaming software integrated by Red Lane B.V. may be independently evaluated and certified by internationally recognised testing laboratories, including, but not limited to:

- Gaming Laboratories International (GLI)
- iTech Labs
- eCOGRA
- BMM Testlabs
- QUINEL
- SIQ Gaming Laboratories

Scope of Certification

Independent certification covers, where applicable:

- Random Number Generator (RNG) implementation;
- Statistical randomness and distribution;
- Game mathematics;
- Return to Player (RTP) verification;
- Jackpot calculations;
- Game rules and payout logic;
- Software integrity;
- Source code review (where performed by the testing laboratory);
- Information security controls;
- Transaction processing accuracy;
- Communication security;
- Platform integration testing;

- Technical compliance with applicable regulatory requirements.

Certification confirms that gaming software performs according to its documented specifications and approved mathematical models.

Random Number Generator Certification

For RNG-based games, independent laboratories evaluate whether the implemented RNG produces sufficiently random and statistically independent outcomes. Testing commonly includes:

Statistical Analysis

The laboratory performs extensive statistical analysis using recognised methodologies to evaluate the randomness of generated values. Testing may include:

- Frequency tests;
- Chi-square analysis;
- Serial correlation testing;
- Runs testing;
- Poker testing;
- Gap testing;
- Spectral testing;
- Entropy analysis;
- Distribution analysis.

Millions of simulated game rounds may be analysed to confirm statistical compliance.

Randomness Verification

Testing confirms that:

- Every generated value is independent;
- No predictable sequence exists;
- Previous outcomes do not influence future outcomes;
- Generated values conform to approved probability distributions.

Security Assessment

The testing laboratory evaluates whether the RNG implementation is adequately protected against:

- External manipulation;
- Internal modification;
- Predictable seed values;
- Software tampering;
- Unauthorised access.

Mathematical Certification

Gaming laboratories review the mathematical model used by each game to verify that theoretical performance corresponds with actual gameplay. Certification generally includes verification of:

- Return to Player (RTP);
- House edge;
- Paytable accuracy;
- Winning probability;
- Bonus feature probabilities;
- Jackpot contribution calculations;
- Volatility profile;
- Hit frequency;
- Symbol weighting.

The laboratory confirms that mathematical calculations are correctly implemented within the gaming software.

Functional Certification

Independent testing also verifies that the game functions correctly. Testing may include:

- Game launch;
- Bet placement;
- Spin functionality;
- Card dealing;
- Outcome determination;
- Bonus activation;
- Jackpot triggering;
- Free spin operation;
- Balance updates;
- Win calculations;
- Transaction recording;
- Error handling.

All functions must operate consistently with the published game rules.

Security Certification

Independent laboratories may assess the technical security of gaming software by reviewing:

- Secure communications;
- Data integrity;
- Encryption implementation;
- Authentication mechanisms;
- Session management;
- Input validation;
- Protection against unauthorised modification;
- Software deployment controls.

The objective is to minimise operational and cybersecurity risks affecting gaming integrity.

Return to Player (RTP) Verification

The testing laboratory verifies that each game's theoretical RTP corresponds with the approved mathematical model. Verification typically involves:

- Large-scale automated simulations;
- Mathematical analysis;
- Statistical validation;
- Comparison with published RTP values.

Only RTP configurations approved by the provider and permitted under the applicable regulatory framework are deployed.

Certification Prior to Deployment

Before integrating a new gaming provider or game portfolio, Red Lane B.V. performs due diligence to confirm that:

- The provider is appropriately licensed or authorised within its operating jurisdiction;
- The gaming software has been independently tested and certified where required;
- Technical documentation is available where appropriate;
- The provider maintains recognised information security and operational controls.

Where certification documentation is provided by the supplier, the Company retains copies as part of its compliance records.

15. Data Centre and Physical Security

Purpose

The purpose of this section is to describe the high-level data centre and physical security arrangements supporting the information technology infrastructure of Red Lane B.V. The Company recognises that secure hosting infrastructure is fundamental to maintaining the confidentiality, integrity, and availability of gaming systems, customer information, financial records, and regulatory data.

Red Lane B.V. utilises reputable third-party cloud hosting and infrastructure providers that maintain industry-recognised security standards and operate professionally managed data centres. While the physical operation and security of these facilities remain the responsibility of the hosting providers, the Company performs appropriate due diligence before selecting infrastructure partners and implements complementary logical, operational, and governance controls to safeguard its services.

Hosting Infrastructure

The Red Lane B.V. gaming platform is hosted using secure cloud and infrastructure services provided by established technology providers, including cloud environments and dedicated hosting solutions such as **Amazon Web Services (AWS)** and network infrastructure providers such as **Voxility**, where applicable.

These providers deliver enterprise-grade hosting services designed to support:

- High system availability;
- Network resilience;
- Scalability;
- Secure data processing;
- Redundant infrastructure;
- Disaster recovery capabilities;
- Continuous operational monitoring.

The Company selects infrastructure providers based on technical capability, operational reliability, information security practices, and their ability to support regulatory and business continuity requirements.

Physical Security Responsibilities

The physical security of the hosting facilities is managed by the respective cloud or data centre provider. Red Lane B.V. does not own or directly operate the physical data centres in which its infrastructure is hosted.

Accordingly, responsibility for physical site security — including building access, environmental controls, power infrastructure, fire protection, surveillance systems, and facility operations — rests with the hosting provider.

The Company relies on the provider's documented security controls, certifications, and contractual commitments when selecting and maintaining hosting services.

Expected Physical Security Controls

Red Lane B.V. expects its hosting providers to implement appropriate physical security measures consistent with recognised industry standards. These controls typically include:

- Restricted access to data centre facilities;
- Multi-layer physical access controls;
- Identity verification for authorised personnel;
- Electronic access logging;
- Continuous CCTV monitoring of sensitive areas;
- Intrusion detection and alarm systems;
- On-site security personnel where appropriate;
- Visitor management procedures;
- Secure equipment handling and disposal processes.

These measures are intended to minimise the risk of unauthorised physical access to critical infrastructure.

Environmental Protection

Hosting providers are expected to maintain suitable environmental controls to protect hardware and networking equipment from operational risks. Such controls may include:

- Climate-controlled environments;
- Fire detection systems;
- Fire suppression systems;
- Water leak detection;
- Temperature and humidity monitoring;
- Uninterruptible Power Supplies (UPS);
- Backup generators;
- Redundant power distribution;
- Redundant cooling systems.

These controls help ensure continuous operation of critical services.

Infrastructure Redundancy

The hosting infrastructure supporting Red Lane B.V. is designed to minimise service interruptions through the use of redundant technology components where appropriate. Infrastructure resilience may include:

- Redundant network connectivity;
- Multiple internet transit providers;
- Load balancing;
- Redundant storage systems;
- High-availability server architecture;
- Automated failover mechanisms;
- Geographic redundancy where supported by the provider.

These measures assist in maintaining platform availability during component failures or maintenance activities.

Network Security

In addition to the physical protections implemented by the hosting provider, Red Lane B.V. implements logical security measures to protect its hosted environment. These controls include:

- Network segmentation;
- Secure firewall configurations;
- Intrusion detection and prevention systems;
- DDoS protection where available;
- Secure VPN access for authorised administrators;
- Network monitoring;
- Encrypted communications;
- Continuous security logging.

Logical security controls complement the physical protections provided by the hosting infrastructure.

16. GDPR Compliance and Data Protection Principles

Purpose

The purpose of this section is to describe the data protection framework implemented by **Red Lane B.V.** to ensure that personal data relating to players, employees, business partners, and other stakeholders is processed lawfully, fairly, securely, and transparently.

Red Lane B.V. recognises the importance of protecting personal information and maintaining the confidentiality, integrity, and availability of all personal data processed through its online gaming operations. The Company applies data protection principles consistent with:

- The **General Data Protection Regulation (EU) 2016/679 (GDPR)** where applicable;
- Applicable Curaçao data protection requirements;
- The requirements of the Curaçao Gaming Authority (CGA);
- Internationally recognised information security and privacy standards.

Data Protection Governance Framework

Red Lane B.V. maintains a structured data protection framework designed to ensure that personal data is managed responsibly throughout its lifecycle. The framework includes:

- Defined responsibilities for data protection management;
- Internal data handling procedures;
- Information security controls;
- Access management restrictions;
- Data retention procedures;
- Incident response processes;
- Employee confidentiality obligations;
- Third-party data processing oversight.

The Company applies a privacy-by-design and privacy-by-default approach when implementing new systems, processes, and services.

Roles and Responsibilities

Board of Directors / Senior Management

Senior Management is responsible for ensuring that appropriate resources, governance structures, and controls are implemented to protect personal data. Responsibilities include:

- Approving data protection policies;
- Supporting compliance initiatives;
- Ensuring appropriate risk management;
- Reviewing significant data protection incidents.

Data Protection Responsible Person

Red Lane B.V. designates responsible personnel to oversee data protection compliance activities. Responsibilities include:

- Monitoring compliance with applicable privacy requirements;
- Advising internal departments regarding data protection matters;
- Reviewing privacy risks;
- Coordinating responses to data subject requests;
- Supporting incident investigations;
- Maintaining data protection documentation.

Employees and Contractors

All employees and contractors handling personal information must:

- Maintain confidentiality;
- Follow approved data handling procedures;
- Use information only for authorised purposes;
- Report suspected security incidents;
- Complete required data protection training.

Categories of Personal Data Processed

During the operation of its online gaming services, Red Lane B.V. may process various categories of player information, including:

Identification Data

- Full name;
- Date of birth;
- Nationality;
- Government-issued identification information;
- Identity verification documents.

Contact Information

- Email address;
- Telephone number;
- Residential address;
- Communication records.

Financial Information

- Deposit information;
- Withdrawal information;
- Payment transaction records;
- Banking details;
- Payment method information.

Gaming Activity Information

- Betting history;
- Gaming sessions;
- Deposits and withdrawals;
- Bonuses received;
- Account activity;
- Responsible Gaming indicators.

Technical Information

- IP address;
- Device information;
- Browser information;
- Login history;
- Security logs;
- Session information.

Lawful Basis for Processing Personal Data

Red Lane B.V. processes personal data only where a lawful basis exists. Processing activities may rely on:

Contractual Necessity

Personal data is processed to provide gaming services requested by players, including:

- Account creation;
- Gaming access;
- Payment processing;
- Customer support.

Legal and Regulatory Obligations

Personal data may be processed to satisfy regulatory requirements, including:

- AML/CFT obligations;
- Customer identification requirements;
- Financial record keeping;
- Regulatory reporting.

Legitimate Interests

Processing may occur where necessary for legitimate business purposes, including:

- Fraud prevention;
- Platform security;
- Service improvement;
- Technical monitoring.

Consent

Where required, the Company obtains explicit consent from users before processing certain categories of information.

Data Protection Principles

Red Lane B.V. follows the core GDPR data protection principles.

Principle 1: Lawfulness, Fairness and Transparency

The Company ensures that personal data is:

- Processed lawfully;
- Used fairly;
- Explained clearly to players.

Players receive information through:

- Privacy Policy;
- Terms and Conditions;
- Account notices;
- Consent mechanisms.

Principle 2: Purpose Limitation

Personal data is collected only for specific and legitimate purposes. Examples include:

- Providing gaming services;
- Verifying player identity;
- Processing payments;
- Preventing fraud;
- Meeting AML requirements.

Personal data is not used for unrelated purposes without appropriate justification.

Principle 3: Data Minimisation

Red Lane B.V. collects only information necessary for operational, legal, regulatory, and security purposes. The Company avoids collecting unnecessary personal information.

Principle 4: Accuracy

The Company maintains procedures to ensure that personal information remains accurate and up to date. Players may update certain account information through their account profile or by contacting Customer Support.

Principle 5: Storage Limitation

Personal data is retained only for as long as necessary for:

- Business operations;
- Legal obligations;
- Regulatory requirements;
- Dispute management;
- Fraud prevention.

After the retention period expires, information is securely deleted or anonymised.

Principle 6: Integrity and Confidentiality

Red Lane B.V. protects personal data through appropriate technical and organisational measures. Controls include:

- Encryption;
- Access restrictions;
- Authentication controls;
- Monitoring;
- Audit logging;
- Secure storage;
- Confidentiality obligations.

Principle 7: Accountability

The Company maintains evidence demonstrating compliance with applicable data protection obligations. Records may include:

- Policies;
- Procedures;
- Training records;
- Security assessments;
- Processing records;
- Incident documentation.

Player Rights

Red Lane B.V. respects applicable data subject rights, including:

- **Right of Access** — Players may request confirmation of whether their personal data is processed and obtain relevant information.
- **Right to Rectification** — Players may request correction of inaccurate or incomplete information.
- **Right to Erasure** — Players may request deletion of personal information where legally permitted. The Company may retain information where required by AML obligations, regulatory requirements, or legal proceedings.
- **Right to Restriction** — Players may request limitation of processing in certain circumstances.
- **Right to Data Portability** — Where applicable, players may request their personal information in a structured format.
- **Right to Object** — Players may object to certain processing activities where applicable.

Data Security Measures

Red Lane B.V. implements technical and organisational measures including:

Encryption

Protection of information through:

- Encryption of data transmission;

- Secure communication protocols;
- Database security controls.

Access Control

Access to personal data is restricted based on:

- Job responsibilities;
- Minimum necessary access;
- Role-based permissions.

Authentication Security

- Strong passwords;
- Multi-factor authentication where appropriate;
- Account monitoring;
- Access logging.

Monitoring and Logging

Systems maintain records of:

- Login attempts;
- Administrative activity;
- Security events;
- Data access activity.

Data Processing by Third Parties

Red Lane B.V. may engage third-party providers that process personal data on behalf of the Company. Examples include:

- Gaming providers;
- Payment providers;
- Hosting providers;
- Customer support providers;
- Identity verification providers.

Before engagement, third parties are assessed regarding:

- Security capabilities;
- Data protection practices;
- Confidentiality obligations;
- Regulatory suitability.

Contractual arrangements define processing responsibilities, security requirements, confidentiality obligations, and data handling restrictions.

International Data Transfers

Where personal data is transferred internationally, Red Lane B.V. applies appropriate safeguards to ensure that personal information remains protected. Controls may include:

- Contractual protections;
- Provider security assessments;
- Restricted access arrangements;
- Data processing agreements.

Data Breach Management

Red Lane B.V. maintains procedures for identifying, investigating, managing, and responding to personal data breaches. A data breach may include:

- Unauthorised access;
- Loss of personal information;
- Accidental disclosure;
- Security compromise.

Incident response procedures include:

1. Detection and containment;
2. Risk assessment;
3. Investigation;
4. Remediation;
5. Documentation;
6. Regulatory notification where required;
7. Communication with affected parties where appropriate.

Employee Training

Employees handling personal data receive appropriate training covering:

- Data protection principles;
- Confidentiality obligations;
- Secure information handling;
- Phishing awareness;
- Incident reporting;
- Access control requirements.

Training records are maintained as evidence of compliance.

Privacy by Design and Default

Red Lane B.V. integrates privacy considerations into the development and operation of its systems. Examples include:

- Collecting only necessary information;
- Restricting access by role;
- Applying security controls during system design;
- Protecting player privacy settings by default.

Regulatory Cooperation

Red Lane B.V. cooperates with competent authorities, including the Curaçao Gaming Authority, where required. The Company maintains appropriate documentation demonstrating:

- Data protection governance;
- Security measures;
- Operational procedures;
- Compliance controls.

17. Secure Deletion (as part of data retention)

Purpose

The purpose of this section is to define the secure data deletion procedures implemented by **Red Lane B.V.** to ensure that personal data, confidential information, and operational records are securely removed when they are no longer required for business, regulatory, legal, or security purposes.

Red Lane B.V. recognises that secure deletion is an essential component of effective data lifecycle management and is necessary to ensure compliance with:

- Applicable data protection requirements;
- The General Data Protection Regulation (GDPR), where applicable;
- Curaçao Gaming Authority (CGA) expectations;
- Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT/CPF) obligations;
- Internal information security requirements.

The Company ensures that information is not retained indefinitely and that expired data is securely deleted, anonymised, or rendered permanently inaccessible.

Scope

These secure deletion procedures apply to all categories of information processed by Red Lane B.V., including:

- Player personal data;
- Customer identification records;
- KYC documentation;
- Payment and transaction records;
- Gaming activity records;
- Account information;
- Communication records;
- Responsible Gaming records;
- Fraud monitoring information;
- AML/CFT records;
- Employee and contractor information;
- Business partner information;
- System logs;
- Technical records;
- Electronic documents and databases.

The procedures apply to information stored within:

- Production databases;
- Application systems;
- Cloud hosting environments;

- Backup systems;
- File storage platforms;
- Internal company systems;
- Third-party processing environments.

Data Lifecycle Management Principles

Red Lane B.V. applies a structured data lifecycle approach consisting of:

1. Data collection;
2. Data classification;
3. Data storage;
4. Data usage;
5. Data retention;
6. Data review;
7. Secure deletion or anonymisation.

Personal data is deleted only after confirming that:

- The retention period has expired;
- No legal obligation requires continued retention;
- No regulatory investigation is ongoing;
- No dispute, complaint, or legal proceeding requires preservation.

Data Retention Review Process

Before deletion is initiated, the Company performs a retention review. The review considers:

- Applicable legal requirements;
- AML/CFT retention obligations;
- Regulatory requirements;
- Contractual obligations;
- Pending investigations;
- Litigation requirements;
- Business requirements.

Records subject to legal holds or regulatory review are excluded from deletion until the relevant restriction is removed.

Data Classification Before Deletion

Information is classified before disposal to ensure appropriate handling. Categories include:

Customer Identification Information

- Name;
- Date of birth;
- Identity documents;

- Address verification documents.

Financial Records

- Deposits;
- Withdrawals;
- Payment confirmations;
- Transaction histories.

Gaming Records

- Bets;
- Game sessions;
- Results;
- Account activity.

Compliance Records

- AML investigations;
- Suspicious transaction reports;
- Customer risk assessments.

Technical Information

- Logs;
- System records;
- Access information.

Each category follows the appropriate retention and deletion procedure.

Secure Electronic Data Deletion

Electronic information is deleted using controlled procedures designed to prevent unauthorised recovery. Deletion methods may include:

- Secure database deletion;
- Permanent record removal;
- Cryptographic erasure;
- Secure overwrite procedures;
- Storage media sanitisation;
- Account deactivation followed by permanent removal where applicable.

Standard operating system deletion methods are not considered sufficient for sensitive information unless combined with appropriate security controls.

Database Record Deletion Procedures

For information stored within databases, deletion is performed through authorised administrative procedures. The process includes:

1. Identification of records eligible for deletion;
2. Verification of retention expiry;
3. Approval by authorised personnel;
4. Execution of deletion procedure;
5. Confirmation that records are removed;
6. Recording of deletion activity.

Database deletion activities are logged where technically possible.

Customer Account Data Deletion

When a player account reaches the end of its retention period or deletion is legally permitted, Red Lane B.V. may perform the following actions:

- Remove unnecessary personal information;
- Delete inactive account information;
- Remove stored documents where legally permitted;
- Anonymise historical statistical data;
- Disable access credentials;
- Remove personal identifiers from operational systems.

Where records must be retained due to legal obligations, the information is restricted and securely stored until the retention period expires.

KYC Document Secure Deletion

Identity verification documents are treated as highly sensitive information. Before deletion:

- Retention requirements are verified;
- Compliance approval is obtained where required;
- Documents are permanently removed from active storage;
- Access permissions are reviewed;
- Deletion activity is recorded.

Copies stored in temporary locations, shared folders, or working environments are also identified and removed.

AML/CFT Record Deletion

AML/CFT records are not deleted before the expiry of mandatory retention periods. This includes:

- Customer due diligence records;
- Risk assessments;
- Transaction monitoring records;
- Investigation files;
- Suspicious activity documentation.

Deletion is performed only after confirmation that:

- The statutory retention period has expired;
- No investigation is pending;

- No regulator requires continued access.

Backup Data Deletion

Red Lane B.V. recognises that deleting information from live systems does not automatically remove it from backup environments. Backup deletion procedures include:

- Applying defined backup retention periods;
- Automatic expiration of backup files;
- Secure destruction of expired backups;
- Prevention of unauthorised restoration;
- Monitoring of backup lifecycle processes.

Where immediate deletion from backups is technically impractical, appropriate access restrictions and security controls are applied until scheduled backup destruction occurs.

Cloud Storage Deletion

Where information is stored within cloud environments, Red Lane B.V. relies on secure deletion mechanisms provided by its infrastructure providers. Cloud deletion processes may include:

- Permanent removal of stored objects;
- Removal of database records;
- Storage encryption key destruction;
- Secure resource termination;
- Provider-managed media sanitisation.

The Company ensures that cloud providers maintain appropriate security practices through contractual arrangements and due diligence procedures.

Third-Party Data Deletion

Where personal data is processed by third-party providers, Red Lane B.V. ensures that deletion obligations are included within contractual arrangements. Third parties may include:

- Payment providers;
- Gaming providers;
- Hosting providers;
- Customer support providers;
- Identity verification providers.

The Company requires providers to:

- Delete data when instructed;
- Follow applicable retention requirements;
- Confirm completion where necessary;
- Maintain confidentiality after termination.

Physical Document Destruction

Where physical documents exist, secure destruction methods are applied. Examples include:

- Confidential shredding;
- Secure document disposal services;
- Controlled destruction processes.

Physical destruction is performed to prevent reconstruction or unauthorised access.

Access Control During Deletion

Deletion activities are restricted to authorised personnel. Controls include:

- Role-based permissions;
- Administrator approval;
- Authentication requirements;
- Activity logging;
- Separation of duties.

Employees are prohibited from independently deleting regulated or sensitive records without appropriate authorisation.

Deletion Verification

Following deletion, Red Lane B.V. performs verification checks where appropriate. Verification may include:

- Database confirmation;
- Storage review;
- Backup lifecycle confirmation;
- Access testing;
- System audit review.

The objective is to ensure that information has been removed or appropriately anonymised.

18. Elements of Visual Representation (Entertainment / Transparency / Player Protection)

Purpose

The purpose of this section is to describe the visual representation principles implemented by **Red Lane B.V.** across its online gaming platform to ensure that the presentation of gambling services is:

- Clear and understandable;
- Transparent to players;
- Fair and non-misleading;
- Consistent with responsible gambling principles;
- Designed to support informed player decisions.

Red Lane B.V. recognises that the visual presentation of an online gambling platform plays an important role in protecting players and ensuring compliance with regulatory expectations established by the **Curaçao Gaming Authority (CGA)**.

The Company ensures that all visual elements, user interfaces, promotional materials, gaming displays, and player information sections are designed to provide an appropriate balance between entertainment value, transparency, and player protection.

General Visual Design Principles

The Red Lane platform applies the following core principles:

Clarity

Information presented to players must be easily understandable and accessible. Examples:

- Clear navigation menus;
- Easily identifiable account sections;
- Visible payment information;
- Clear bonus terms;
- Accessible Responsible Gaming tools.

Accuracy

All visual representations must accurately reflect the actual services offered. The Company prohibits:

- Misleading game descriptions;
- False promotional statements;
- Incorrect payout information;
- Hidden material conditions.

Fair Presentation

The platform design must not encourage excessive gambling behaviour or create unrealistic expectations. The Company ensures that:

- Winning outcomes are not guaranteed or exaggerated;
- Promotional content is presented responsibly;
- Risks associated with gambling remain visible.

Entertainment Elements

Purpose of Entertainment Features

The Red Lane platform provides entertainment-focused gaming experiences while maintaining responsible gaming standards. Entertainment elements are designed to improve usability, engagement, and enjoyment without encouraging irresponsible gambling behaviour.

Gaming Interface Design

Gaming interfaces may include:

- High-quality graphics;
- Game animations;
- Interactive features;
- Sound effects;
- Visual themes;
- Game information panels;
- Achievement displays.

These elements are designed to enhance the player experience while ensuring that the underlying gambling activity remains transparent.

Game Categories and Navigation

The platform provides clear categorisation of gambling products, including:

- Casino Games;
- Slots;
- Live Casino;
- Table Games;
- Sportsbook;
- Virtual Sports;
- Esports.

Players can easily identify available products through organised menus and search functionality.

Promotional Entertainment Features

Where promotional features are offered, such as bonuses, free spins, loyalty rewards, tournaments, and VIP programmes, the Company ensures that:

- Eligibility requirements are clearly displayed;
- Terms and conditions are accessible;

- Restrictions are disclosed before participation.

Promotional features are not designed to create misleading impressions of guaranteed winnings.

Mobile User Experience

The platform is designed to provide consistent functionality across desktop computers, mobile browsers, tablets, and different screen sizes. The mobile interface maintains access to:

- Account management;
- Responsible Gaming tools;
- Payment information;
- Customer support;
- Terms and conditions.

Transparency Elements

Purpose

Transparency is a fundamental requirement of Red Lane B.V.'s gaming operations. The Company ensures that players receive sufficient information to understand:

- The nature of gambling activities;
- Rules of games;
- Financial transactions;
- Promotional conditions;
- Account status.

Game Information Disclosure

Each game presentation provides, where applicable:

- Game name;
- Game provider;
- Rules of play;
- Betting limits;
- Paytable information;
- Winning combinations;
- RTP information where available;
- Bonus feature explanations.

Players must have access to sufficient information before participating.

Betting and Financial Transparency

The platform clearly displays:

- Minimum and maximum betting limits;
- Available balance;
- Deposit amounts;

- Withdrawal amounts;
- Transaction history;
- Bonus balances;
- Wagering requirements where applicable.

Players are able to review their financial activity through their account interface.

Bonus Transparency

All bonuses and promotional offers include clear information regarding:

- Eligibility criteria;
- Expiry dates;
- Minimum requirements;
- Wagering conditions;
- Maximum winnings where applicable;
- Withdrawal restrictions.

The Company avoids presenting bonuses in a manner that could mislead players.

Terms and Conditions Accessibility

The platform provides visible access to:

- Terms and Conditions;
- Privacy Policy;
- Responsible Gaming Policy;
- Complaint Procedures;
- AML-related information where applicable.

Players are required to accept applicable terms before using gambling services.

Outcome Transparency

Players are provided with information explaining:

- How game outcomes are determined;
- The role of RNG systems;
- The difference between games of chance and skill-based activities;
- Settlement procedures.

The Company does not suggest that players can influence random outcomes.

Player Protection Elements

Purpose

Red Lane B.V. incorporates player protection features into the visual design and operation of its platform to support responsible gambling and reduce gambling-related risks.

Responsible Gaming Visibility

Responsible Gaming information is displayed in an accessible manner. Players can access:

- Responsible Gaming policy;
- Information about gambling risks;
- Self-assessment tools;
- Self-exclusion options;
- Deposit limits;
- Cooling-off periods;
- Customer support contacts.

Age Restriction Display

The platform clearly communicates that gambling services are restricted to eligible adults. Visual controls include:

- Age restriction notices;
- Registration verification requirements;
- Responsible gambling warnings.

Players must complete required age and identity verification procedures before full access is provided.

Account Status Information

Players can view important account information, including:

- Current balance;
- Deposit history;
- Withdrawal status;
- Betting activity;
- Bonus status.

This supports informed decision-making.

Responsible Gaming Tools Presentation

The platform provides visible access to player protection tools, including:

Deposit Limits

Players may establish restrictions on deposits according to available Responsible Gaming functionality.

Cooling-Off Periods

Players may temporarily suspend gambling activity for a defined period.

19. Terms and Conditions

Purpose

The purpose of this section is to describe the Terms and Conditions ("T&C") framework implemented by **Red Lane B.V.** for the operation of the **Portobahis** online gaming platform.

The Terms and Conditions establish the contractual relationship between Red Lane B.V. and players accessing and using the Company's online gambling services.

The Terms and Conditions are designed to ensure that players receive clear, transparent, and understandable information regarding:

- The rules governing use of the platform;
- Player obligations and responsibilities;
- Available gaming services;
- Account management requirements;
- Deposits and withdrawals;
- Bonuses and promotions;
- Responsible Gaming requirements;
- Complaints and dispute procedures;
- Legal and regulatory obligations.

Red Lane B.V. ensures that the Terms and Conditions are easily accessible to players before registration and throughout their relationship with the Company.

20. File Contents and Digital Record Management Framework

Purpose

The purpose of this section is to define the categories, structure, content, storage requirements, and management procedures applicable to digital records maintained by **Red Lane B.V.**

Red Lane B.V. recognises that maintaining complete, accurate, secure, and retrievable digital records is a fundamental requirement for:

- Operational integrity;
- Regulatory compliance;
- Audit readiness;
- Player protection;
- AML/CFT/CPF compliance;
- Data protection obligations;
- Business continuity.

This section establishes the framework governing the creation, storage, protection, retention, retrieval, and disposal of digital records generated through the operation of the **Portobahis** online gaming platform.

Scope

This framework applies to all electronic records generated, received, processed, or stored by Red Lane B.V., including:

- Player records;
- Gaming records;
- Financial records;
- Compliance records;
- Regulatory records;
- Technical records;
- Security records;
- Corporate records;
- Employee records;
- Third-party provider documentation.

Digital records may be stored within:

- Gaming platform databases;
- Cloud infrastructure environments;
- Secure document management systems;
- Compliance management systems;
- Internal corporate storage systems;
- Approved third-party systems.

Digital Record Classification

Red Lane B.V. classifies digital records according to their nature, sensitivity, and regulatory importance. Records are classified into the following categories:

1. Player and Customer Records;
2. Gaming Activity Records;
3. Financial and Transaction Records;
4. AML/CFT/CPF Compliance Records;
5. Responsible Gaming Records;
6. Regulatory and Licensing Records;
7. Technical and Infrastructure Records;
8. Security and Audit Records;
9. Corporate and Administrative Records;
10. Third-Party Provider Records.

Player and Customer Records

Customer Registration Information

The Company maintains digital records relating to player registration activities, including:

- Player username;
- Customer identification number;
- Registration date and time;
- Registered email address;
- Telephone number;
- Country of residence;
- Date of birth;
- Account status;
- Account history.

Customer Identification and Verification Records

Where required, the Company maintains KYC documentation, including:

- Identity verification documents;
- Passport or national identification documents;
- Proof of address documents;
- Verification results;
- Verification dates;
- Verification provider records;
- Customer risk classification.

These records support compliance with AML/CFT and customer identification requirements.

Gaming Activity Records

Red Lane B.V. maintains digital records relating to player gaming activity.

Betting Records

- Bet placement date and time;
- Game or event identifier;
- Stake amount;
- Odds;
- Potential winnings;
- Settlement result;
- Transaction reference.

Casino Game Records

- Game title;
- Game provider;
- Session information;
- Number of rounds played;
- Bets placed;
- Wins and losses;
- Game outcomes;
- Bonus activity.

Sportsbook Records

- Sporting event;
- Market selection;
- Odds;
- Stake;
- Settlement information;
- Result determination source.

Live Casino Records

- Game type;
- Session information;
- Bet history;
- Dealer/game reference;
- Settlement information.

Financial and Transaction Records

The Company maintains complete digital records relating to all financial activity.

Deposit Records

- Player account identifier;

- Payment method;
- Amount deposited;
- Currency;
- Date and time;
- Payment provider;
- Transaction reference;
- Status.

Withdrawal Records

- Withdrawal request date;
- Amount;
- Payment destination;
- Verification status;
- Approval status;
- Processing date;
- Transaction reference.

Payment Provider Records

- Provider details;
- Transaction confirmations;
- Failed transactions;
- Chargebacks;
- Refund records.

AML/CFT/CPF Compliance Records

Red Lane B.V. maintains dedicated compliance records required for AML/CFT/CPF purposes.

Customer Due Diligence Records

- Customer identification information;
- Verification documentation;
- Customer risk assessment;
- KYC review history.

Enhanced Due Diligence Records

- High-risk customer assessments;
- Source of Funds documentation;
- Source of Wealth information;
- Approval records.

Transaction Monitoring Records

- Monitoring alerts;

- Investigation notes;
- Analyst reviews;
- Escalation records;
- Final decisions.

Suspicious Transaction Records

- Internal reports;
- Investigation files;
- Regulatory submissions where applicable;
- Supporting documentation.

Responsible Gaming Records

The Company maintains records supporting responsible gambling obligations. These include:

- Self-assessment results;
- Deposit limit requests;
- Cooling-off requests;
- Self-exclusion requests;
- Player interactions;
- Responsible Gaming communications;
- Intervention records.

Regulatory and Licensing Records

Red Lane B.V. maintains digital documentation supporting its regulatory obligations.

Licensing Documentation

- Gaming licence documentation;
- Regulatory correspondence;
- Applications;
- Approvals;
- Renewals.

Policies and Procedures

- AML/CFT Policy;
- Responsible Gaming Policy;
- Data Protection Policy;
- Complaint Policy;
- Security Policies;
- Operational Manual.

Regulatory Communications

- Correspondence with CGA;

- Regulatory submissions;
- Compliance responses;
- Inspection documentation.

Technical and Infrastructure Records

The Company maintains technical records necessary for operational reliability.

System Documentation

- Platform architecture;
- Integration documentation;
- API documentation;
- System configurations.

Infrastructure Records

- Hosting information;
- Server configurations;
- Network documentation;
- Disaster recovery information.

Software Records

- Software versions;
- Release documentation;
- Change requests;
- Deployment records.

Security and Audit Records

Red Lane B.V. maintains security-related digital records including:

- User access logs;
- Authentication records;
- Administrative activity logs;
- Security alerts;
- Incident reports;
- Vulnerability assessments;
- Penetration testing results;
- Audit findings;
- Remediation actions.

Corporate and Administrative Records

Corporate records maintained electronically include:

- Company registration documents;

- Shareholder information;
- Director information;
- Agreements;
- Contracts;
- Supplier documentation;
- Internal approvals;
- Meeting records.

Third-Party Provider Records

Records relating to external service providers include:

- Supplier agreements;
- Gaming provider contracts;
- Payment provider contracts;
- Hosting provider agreements;
- Due diligence documentation;
- Certification documents;
- Service-level agreements.

File Structure and Organisation

Digital records are organised using controlled folder structures and logical categorisation. Example structure:

```
Red Lane B.V.  
01 Corporate Documents  
02 Licensing & Regulatory  
03 AML-CFT Compliance  
04 Player Records  
05 Financial Records  
06 Gaming Operations  
07 Responsible Gaming  
08 Technical Infrastructure  
09 Security & Audit  
10 Third-Party Providers  
11 Policies & Procedures  
12 Incident Management
```

Access to each category is restricted according to employee responsibilities.

File Integrity and Authenticity Controls

Red Lane B.V. implements controls to maintain the integrity of stored records. Controls include:

- Access restrictions;
- Version control;
- Audit logging;

- Document approval workflows;
- Backup procedures;
- Encryption;
- Controlled modification rights.

Unauthorised alteration or deletion of regulated records is prohibited.

Digital Record Access Controls

Access to digital records is managed according to the principle of least privilege. Controls include:

- Individual user accounts;
- Role-based access permissions;
- Authentication requirements;
- Access reviews;
- Administrator monitoring.

Only authorised personnel may access sensitive information.

Backup and Recovery of Digital Records

Digital records are protected through backup procedures designed to ensure availability and recovery. Backup controls include:

- Regular automated backups;
- Secure backup storage;
- Backup monitoring;
- Recovery testing;
- Restricted backup access.

Record Retention

Digital records are retained according to:

- Regulatory requirements;
- AML/CFT obligations;
- Data protection requirements;
- Legal obligations;
- Business requirements.

Retention periods are reviewed periodically.

Secure Deletion

After expiration of applicable retention periods, digital records are securely deleted or anonymised according to the Company's Secure Deletion Procedures. Deletion activities are controlled and documented.

Regulatory Access and Availability

Red Lane B.V. ensures that required digital records can be retrieved promptly for:

- Internal review;
- Audit purposes;
- Regulatory inspection;
- CGA requests;
- Legal proceedings.

Records are maintained in a format that ensures:

- Readability;
- Accuracy;
- Completeness;
- Availability.

09.07.2026

The document is prepared by Portobahis management