

OPERATIONS MANUAL DRAFT

Trigonon Group N.V. | www.goal365.bet | Version 1.0 — DRAFT | July 2026

Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao — Company No. 142028

Licensed by the Curaçao Gaming Authority under license number **OGL/2024/659/0586**, granted on 23 May 2025, in accordance with the National Ordinance on Games of Chance (Landsverordening op de kansspelen, PB 2024 no. 157, the "LOK"/"NOGC").

Document Control

Field	Detail
Document title	Operations Manual — Trigonon Group N.V.
Version	1.0 — Draft
Document date	July 2026
Status	Draft — for Board review. Not approved; not in force.
Owner	NOGC Compliance Officer
Approved by	Not yet approved — approval by the Board of Directors, Trigonon Group N.V., pending
Date of Board approval	Not applicable — Board approval pending
Effective date	Not applicable — no effective date applies while the document is in draft. The effective date will be set by the Board on approval.
Next scheduled review	Annually from the effective date, once set — and earlier after any material legal, regulatory, organisational, system or supplier change, or after a material incident
Licensed operation	www.goal365.bet
CGA license number	OGL/2024/659/0586
License granted	23 May 2025 — status: Active
Classification	Internal — may be provided to the CGA, approved auditors, ADR providers and independent experts
Regulatory basis	LOK/NOGC; CGA online gaming license conditions (indefinite-term, effective 17 December 2025); NORUT; NOIS; SNO; CGA Responsible Gaming Policy v1.0 (17 April 2025); CGA Player Complaints Policy Guidelines v1.1 (18 June 2025); CGA AML/CFT/CPF Regulations (January 2025); CGA Compliance Officer Requirements; CGA Information Security Control Requirements (CIS IG1)

Purpose of this Manual

This Manual is the single operational reference for the licensed operation of **www.goal365.bet**. It describes what the Company does, who does it, when, and against which regulatory requirement. It sits above the individual policies published by the Company and below the LOK and the license conditions.

Contents

Document Control	1
Purpose of this Manual	1
Contents	2
1. Purpose, Scope and Regulatory Framework	6
1.1 Purpose	6
1.2 Scope	6
1.3 Regulatory framework	6
1.4 Document hierarchy	7
2. The Licensed Operation	8
2.1 Company and license particulars	8
2.2 Restriction on activities	8
2.3 Prohibited and restricted markets	8
3. Governance, Key Persons and Organisation	9
3.1 Board accountability	9
3.2 Key persons and roles	9
3.3 Compliance Officer — fit, proper and independent	9
3.4 Segregation of duties	10
3.5 Training	10
4. Customer Identification and Verification	11
4.1 Registration	11
4.1.1 Registration validation sequence	11
4.2 Verification stages and player privileges	11
4.3 Prevention of underage gambling	11
4.4 Customer Due Diligence (CDD)	12
4.4.1 Identity data verified	12
4.4.2 Accepted documents	12
4.4.3 Consequences of incomplete CDD at threshold	12
4.5 Enhanced Due Diligence (EDD)	12
4.6 Politically Exposed Persons	13
4.7 Sanctions screening	13
4.8 Ongoing monitoring and re-verification	13
4.9 Records	13
5. Player Account and Fund Management	14
5.1 One account per player	14
5.2 Information available in the player account	14
5.3 Payment transactions	14
5.4 Segregation of player funds and liquidity	14
5.5 Withdrawals and payouts	15
5.5.1 Incorrect credits	15
5.6 Refunds and chargebacks	15
5.7 Dormant accounts and inactivity	15
5.8 Bonuses and promotions	15

6. Responsible Gaming	16
6.1 Responsible gaming function	16
6.2 Information accessibility	16
6.2.1 Responsible Gaming section	16
6.2.2 Homepage and Terms & Conditions	16
6.2.3 Mandatory footer content	16
6.3 Player self-assessment	16
6.4 Behaviour tracking and intervention	16
6.4.1 Key monitoring indicators	17
6.4.2 Detection method	17
6.4.3 Profiling and escalation	17
6.5 Cooling-off	17
6.6 Self-exclusion	18
6.7 Operator-initiated exclusion	18
6.8 Deposit limits	18
6.9 Other limits and reality check	18
6.9.1 Exceptions affecting active wagering	19
6.10 Internet filtering	19
6.11 Advertising and marketing	19
7. AML / CFT / CPF	20
7.1 Objective	20
7.2 AML compliance programme	20
7.3 Risk-based approach	20
7.3.1 Business Risk Assessment	20
7.3.2 Customer Risk Assessment	20
7.4 Customer due diligence	20
7.5 Transaction monitoring	20
7.6 Internal and external reporting	21
7.6.1 Internal reporting	21
7.6.2 External reporting to the FIU	21
7.6.3 Prohibition of disclosure (tipping-off)	21
7.6.4 Blocking and freezing	21
7.7 Employee screening and training	21
7.8 Independent audit	21
7.9 Records	21
8. Information Security	23
8.1 Relationship to the Information Security Policy	23
8.2 Governance of security	23
8.3 Control summary	23
8.4 Availability and continuity of service	24
8.5 Security incidents and CGA notification	24
8.6 CGA data access	24
8.7 Assurance	24
9. Suspension and Closure of Player Accounts	25

9.1 Grounds	25
9.2 Procedure	25
9.3 Reinstatement	25
10. Games, Gaming Equipment and Software Integrity	27
10.1 Certification	27
10.2 Ongoing integrity monitoring	27
10.3 Inventory and maintenance	27
10.4 Sports data and market integrity	27
10.5 Change management	27
11. Suppliers and Outsourcing	28
11.1 Prior CGA approval	28
11.2 Supplier lifecycle	28
12. Player-Facing Transparency	29
12.1 General Terms & Conditions — mandatory content	29
12.2 Publicly accessible information	29
13. Complaints, Disputes and ADR	31
13.1 Definitions	31
13.2 Submission	31
13.3 Resolution timelines	31
13.4 Outcome	31
13.5 Use of artificial intelligence	32
13.6 Alternative Dispute Resolution	32
13.7 Role of the CGA	32
13.8 Records and reporting	32
13.9 Visibility	32
14. Regulatory Reporting and CGA Interaction	33
14.1 Reporting obligations	33
14.2 The 24-hour incident clock	33
14.3 Critical changes requiring prior CGA permission	33
14.4 Portal and checklist	33
15. Business Continuity, Wind-Down and Records	35
15.1 Business continuity	35
15.2 Wind-down	35
15.3 Records and retention	35
16. Compliance Monitoring and Assurance	36
16.1 Three lines	36
16.2 Compliance calendar	36
16.3 Obligations register	36
16.4 Non-compliance	36
16.5 Review and approval	36
Annex A — Roles and Responsibilities Summary	38
Annex B — Key Thresholds and Deadlines	39
Annex C — Requirement to Manual Mapping	40
Annex D — Reference Documents	41

Legislation and license	41
CGA policies and guidelines	41
Company policies published at www.goal365.bet	41
Company internal documents	41

1. Purpose, Scope and Regulatory Framework

1.1 Purpose

Trigonon Group N.V. (the "Company") operates remote games of chance at **www.goal365.bet** under license number **OGL/2024/659/0586** issued by the Curaçao Gaming Authority. This Manual documents the operational processes, controls, responsibilities and reporting obligations by which the Company delivers a **safe, responsible, transparent, verifiable and reliable** offering of games of chance, as required by the LOK.

The Manual serves four purposes:

1. To give staff, contractors and outsourced providers a single authoritative description of how the licensed operation is run.
2. To demonstrate to the CGA that the Company holds, at all times, the policies and procedures required by Article 14 of the license conditions.
3. To provide the evidence trail required by independent experts, approved auditors and ADR providers.
4. To function as the control document against which internal compliance monitoring and the annual review are performed.

1.2 Scope

This Manual applies to:

- all directors, key persons, employees and contractors of the Company;
- the licensed domain **www.goal365.bet**, which is the sole domain approved in the Company's CGA online gaming portal account;
- all gaming verticals offered — sportsbook (pre-match and in-play), casino, live casino, virtual games and any other vertical added from time to time;
- all gaming equipment, gambling interface and application software used in the exploitation; and
- all outsourced services that fall within the Company's regulatory responsibility, including platform, hosting, game content, sports data feed, payment, KYC and security providers.

Outsourcing does not transfer regulatory accountability. Article 3(2) of the license conditions requires the Company to take all appropriate measures to ensure that outsourced activities comply with all applicable laws and regulations.

www.goal365.bet is the only domain operated under license OGL/2024/659/0586. No mirror domains or subdomains are in use. Adding, changing or removing a domain requires prior CGA permission under Article 4.

1.3 Regulatory framework

Instrument	Relevance to this Manual
LOK / NOGC (PB 2024 no. 157)	Primary gaming legislation. Objectives: prevention of fraud and money laundering; protection of players including minors and vulnerable persons; assurance of payment of winnings; prevention of gambling addiction.
CGA online gaming license conditions	Articles 2–15. Article 14 sets the six mandatory policy and procedure areas that form the spine of Sections 4–9 of this Manual.
NORUT (Ordinance on the Notification of Unusual Transactions)	Obligation to report unusual transactions to the FIU without delay.
NOIS (National Ordinance on Identification in Service Provision)	Customer identification and verification obligations.
SNO (Sanctions National Ordinance)	Sanctions screening obligations (UN, EU, OFAC).
CGA Responsible Gaming Policy v1.0	Nine mandatory responsible gaming elements. Drives Section 6.
CGA Player Complaints Policy Guidelines v1.1	Complaint windows, timelines, ADR and biannual reporting. Drives Section 13.
CGA AML/CFT/CPF Regulations (Jan 2025)	Risk-based approach, CDD, Naf. 4,000 threshold, FIU reporting, five-year retention. Drives Section 7.
CGA Compliance Officer Requirements (NOIS/NORUT)	Fit-and-proper, competence and conflict-of-interest rules for the Compliance Officer. Drives Section 3.

Instrument	Relevance to this Manual
CGA Information Security Control Requirements (CIS IG1)	Security baseline. Implemented through the Company's Information Security Policy; summarized in Section 8.
National Ordinance on the Protection of Personal Data	Processing and storage of player personal data (Article 6(3) of the license conditions).

1.4 Document hierarchy

Where documents conflict, the following order of precedence applies:

1. The LOK and other Curaçao legislation.
2. The Company's CGA license conditions and any action points in the CGA portal checklist.
3. CGA policies, guidelines, instructions and portal manuals in force from time to time.
4. Operations Manual.
5. Individual Company policies published at www.goal365.bet.
6. Internal work instructions, runbooks and system configuration.

Where a published policy conflicts with a position stated in this Manual, the position in this Manual prevails. Any inconsistency identified between a published policy and this Manual is reported to the NOGC Compliance Officer and resolved within 30 days, with the published policy updated on the website and, where applicable, re-uploaded to the CGA portal.

2. The Licensed Operation

2.1 Company and license particulars

Item	Detail
Legal name	Trigonon Group N.V.
Registered address	Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao
Chamber of Commerce number	142028
CGA license number	OGL/2024/659/0586
License type	Online gaming license (B2C) for remote games of chance, issued under the LOK
Date license granted	23 May 2025
License status	Active
Licensing authority and supervisor	Curaçao Gaming Authority (CGA)
Licensed domain	www.goal365.bet
Verticals offered	Sportsbook (pre-match and live), Casino, Live Casino, Virtual games, Other games
Player support	support@goal365.bet — live chat and email
Curaçao operational office	Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao
Hosting provider	Amazon Web Services (AWS)
Player funds institution	Finductive Ltd
ADR provider and CGA portal agent	EGIS – FZCO

2.2 Restriction on activities

Under Article 2(5) of the license conditions the Company offers **no goods or services other than the licensed games of chance**. The Company does not offer credit to players for the purpose of wagering, does not operate currency exchange in or outside the player account, does not exchange virtual currency for fiat currency, and does not offer investment alternatives to players. The issuance or purchase of in-game tokens is not affected by this restriction.

2.3 Prohibited and restricted markets

Registration and play are geo-restricted. The registration process checks the customer's country of origin by IP address against the list of permitted jurisdictions before the registration form is accepted.

The Company applies the list of restricted and prohibited jurisdictions maintained and published by the Curaçao Gaming Authority. That list, as in force from time to time, is the Company's operative permitted-market list. The NOGC Compliance Officer checks the CGA list at least quarterly and after any CGA announcement affecting a market, records the date of each check, and ensures that any change is reflected in the platform geo-blocking and payment-method configuration.

3. Governance, Key Persons and Organisation

3.1 Board accountability

The Board of Directors of Trigonon Group N.V. holds overall accountability for the licensed operation, for compliance with the LOK and the license conditions, and for this Manual. The Board:

- approves this Manual and all policies referenced in it;
- receives and considers the annual Responsible Gaming effectiveness report, the periodic AML/CFT compliance reports and the results of independent audits;
- reviews material compliance findings, incidents and overdue remediation at least quarterly;
- ensures that the operation is conducted at all times by persons of impeccable conduct (Article 6(4) of the license conditions); and
- ensures that the Company holds sufficient funds at all times to pay out prize money, with appropriate ring-fencing and segregation (Article 6(5)).

3.2 Key persons and roles

"Key person" has the meaning given in the NOGC and includes the NORUT/NOIS Compliance Officer and the NOGC Compliance Officer. Under Article 4 of the license conditions, **no key person may be appointed, changed or removed without the prior permission of the CGA.**

Role	Core responsibility	Holder
Managing Director (Curaçao)	Day-to-day management of the licensed entity; primary liaison with the CGA.	Gouloud Hammud
NOGC Compliance Officer	Monitors compliance with the LOK and the license conditions; owns this Manual; owns the CGA portal, change reports, incident reports and the compliance calendar.	Ivaylo Stamchev
NORUT/NOIS Compliance Officer (AML/CFT/CPF)	Designs and runs the AML programme; receives internal unusual-transaction reports; files unusual transaction reports to the FIU; owns the business and customer risk assessments; delivers AML training.	Ivaylo Stamchev
24/7 incident coordinator	Receives and escalates incidents and ensures the 24-hour CGA incident report is filed.	+357 96538375

Where a role is shown as held by a member of the Board of Directors, the individual director discharging it is identified in the Board minutes and is notified to the CGA on request.

3.3 Compliance Officer — fit, proper and independent

The AML/CFT Compliance Officer is a designated senior officer at management level who must be able to act independently and must have timely access to customer identification data, CDD information and transaction records. The CGA requires one of the following qualification routes:

- **Education and experience:** at least two years of AML/CFT compliance experience in a reporting role, plus a bachelor's degree or a recognised AML certification (CAMS, AMLFC, or comparable subject to CGA approval); **or**
- **Experience only:** at least four years of AML/CFT compliance experience in a reporting role; **or**
- at least two years in an MLRO or equivalent role in another jurisdiction.

The Company's Compliance Officer is Ivaylo Stamchev, who qualifies under the second route — at least four years of AML/CFT compliance experience in a reporting role. He holds both the NOGC Compliance Officer role and the NORUT/NOIS (AML/CFT/CPF) Compliance Officer role.

The Compliance Officer must complete **at least 10 hours of AML-related training annually**, must have knowledge of the NOIS, the NORUT and CGA AML regulations, and must be familiar with screening against EU and OFAC sanctions lists.

Conflict of interest. The Compliance Officer role may not be combined with the functions of UBO, CEO, CFO, COO, Casino Manager, Slot Manager or any other operational function, and must be separate from the internal audit function. Where the compliance function is outsourced, the responsible manager's CV must be available to the CGA, the outsourcing contract must be producible on request, and that person may not represent more than ten operators in total, including equivalent roles in other jurisdictions.

3.4 Segregation of duties

The following separations are maintained and evidenced:

- Compliance monitoring is separate from internal audit.
- The person who approves a player withdrawal is not the person who executes the payment.
- The person who applies a manual balance adjustment is not the person who approves it; all manual adjustments are logged with reason code, approver and timestamp.
- Responsible gaming interventions are recorded by the Responsible Gaming function, not by commercial or VIP staff acting alone.
- Administrative access to core gaming systems uses separate named administrator accounts, never shared credentials.

Responsible gaming and AML decisions may never be overridden by commercial or VIP staff. Under the CGA Responsible Gaming Policy, using protective interventions to prevent or delay a legitimate player withdrawal is a breach of license conditions.

3.5 Training

Audience	Content	Frequency
All staff and contractors	LOK obligations, code of conduct, confidentiality, information security awareness, incident reporting, tipping-off prohibition	On appointment and at least annually
Customer support, VIP and marketing	Responsible gaming: recognising signs of gambling distress; conducting sensitive structured conversations; directing players to tools and support resources	On appointment and at least annually
All customer-facing and payments staff	AML/CFT/CPF: unusual transaction indicators, internal reporting route, sanctions and PEP screening, prohibition of disclosure	On appointment and at least annually
Compliance Officer	AML-related continuing professional development	At least 10 hours per year
Technical and administrative staff	Role-based security training for higher-risk roles	On appointment and at least annually

Attendance, content, date and assessment result are recorded for every session and retained for at least five years. Training records are produced to the CGA, to independent experts and to auditors on request.

The Compliance Officer supervises the training programme, sets the annual calendar and approves the content and the assessment standard.

4. Customer Identification and Verification

License conditions Article 14(1)(a) — customer identification and verification. Source policies: KYC Policies, Privacy & Management of Personal Data; AML Policy; Account, Pay-outs and Bonuses.

4.1 Registration

A player must register a player account and log in before participating in any remote game of chance (Article 8(1)). Registration collects, as a minimum:

- email address; username; password and password confirmation;
- full name (first name and last name);
- date of birth;
- permanent residential address (street and number, city, postal code, country);
- identity reference number; and
- mobile number (optional).

4.1.1 Registration validation sequence

1. The customer's country of origin is checked by IP address against the permitted-market list. Registration is refused outside permitted markets.
2. The registration form is validated: email, username, identity number and mobile number must each be unique across the player base.
3. Password strength is enforced — minimum 8–10 characters including at least one uppercase letter, one lowercase letter, one number and one special character; the password may not contain the username, email, mobile number, date of birth or identity number.
4. Age is calculated from the declared date of birth. A date of birth indicating a minor causes the registration to be rejected outright.
5. The player confirms by an unticked checkbox that they are over 18 and accepts the General Terms & Conditions and the Complaints Policy.
6. A verification email is sent; where a mobile number is supplied, a six-digit SMS code is issued.
7. Minimum CDD data (name, permanent residential address, date of birth) is captured and **PEP screening and sanctions screening are run at the moment the account is opened**, before any threshold is reached.

4.2 Verification stages and player privileges

Stage	Log in	Play	Deposit	Withdraw
1. Registered, email/mobile not verified	No	No	No	No
2. Email/mobile verified, CDD/EDD pending	Yes	Yes — limited number of bets	Yes — limited deposit amount / limited cumulative deposits	No
3. Fully verified	Yes	Yes	Yes — subject to risk-based EDD	Yes — subject to risk-based EDD

No withdrawal is ever released before CDD is complete. Stage-2 deposit caps must be set below the NAf. 4,000 CDD trigger described at 4.4.

The stage-2 caps are configured on the platform, are set below the NAf. 4,000 threshold described at 4.4, and are reviewed by the Compliance Officer at least annually.

4.3 Prevention of underage gambling

It is prohibited under Article 1.4(d) of the LOK to allow a minor the opportunity to participate in games of chance. The Company applies:

- self-attestation of date of birth plus an explicit over-18 confirmation checkbox at registration;
- automatic rejection of any declared date of birth indicating a person under 18;
- a government-issued photographic identity document check (passport, national identity card or driving license) on reaching the specified thresholds and **in any case before the first withdrawal**;

- secondary checks at the Company's discretion — electronic verification, payment validation, third-party or government database checks, selfie verification — which supplement but never replace the government-issued document requirement.

If the Company becomes aware at any point that a player is a minor, **the account is closed immediately**, the reason for closure is clearly communicated to the minor, all bets are void, deposits are reimbursed and any winnings are forfeited. Records of all age verification processes and their outcomes are retained and made available for regulatory review.

4.4 Customer Due Diligence (CDD)

Because the customer is not physically present, the ML/FT risk is by default high and enhanced measures apply. CDD is completed:

- **always before any withdrawal is released;**
- at the point where cumulative deposits and withdrawals since the start of the relationship reach or exceed **NAf. 4,000**, calculated on a daily basis and including any peer-to-peer transfers; and
- before any deposit above the stage-2 limited amount.

4.4.1 Identity data verified

- official full name;
- date of birth;
- identity reference number;
- permanent residential address;
- nationality.

4.4.2 Accepted documents

Purpose	Accepted documents
Identity, date of birth, ID number, nationality	Valid unexpired passport; valid unexpired national identity card; valid unexpired driving license; valid unexpired residence card
Residential address (issued within the last 6 months, showing full name and address)	Utility bill (water, power, heating); landline communication bill; statement from a recognised credit institution or bank; official conduct certificate; correspondence from a central or local government authority; record of a visit to the address by a senior official; an identity document showing the residential address; any other government-issued document
Not accepted for address	Mobile telephone bills — the residential address is not considered permanent

Verification is made by reference to official documents, data or information obtained from a reliable and independent source — a government authority, department or agency, a regulated utility company, or a subject person carrying out relevant financial business in a jurisdiction applying equivalent standards.

4.4.3 Consequences of incomplete CDD at threshold

Situation	Consequence
NAf. 4,000 reached through deposits	The player may continue to play with funds already in the account but may make no further deposits and no withdrawals until CDD is complete.
NAf. 4,000 reached because the player requests a withdrawal	The account is fully frozen. The player may not continue playing.
Information not received within 30 days of the threshold being reached	The relationship is terminated. If a presumption of ML/FT exists, the transaction is reported to the FIU and internal procedure determines whether funds are blocked, with due regard to the tipping-off prohibition. If no presumption exists, funds are returned to the same bank account or wallet from which they were deposited.

4.5 Enhanced Due Diligence (EDD)

All customers are subject to EDD; the extent and frequency are set by the customer's risk level. EDD is applied **always** on the addition of new payment details (cards, bank accounts, wallets) and **periodically** based on risk. EDD measures include:

1. Obtaining additional identity documentation, over and above the CDD set. Where a document is of the same type as one already held (for example a utility bill), it must be issued by a different entity or service provider.
2. Supplementary verification — certification by a legal or accountancy professional, a notary, or a person undertaking relevant financial business. The certified copy must be a true copy of the original, seen and verified by the certifier, include a photograph of the customer, and carry the certifier's signature, profession, contact details and review date. Certified documents originating from high-risk jurisdictions receive additional scrutiny.
3. Establishing the source of funds and, where indicated by risk, the source of wealth.
4. Enhanced ongoing monitoring of the relationship and its transactions.

4.6 Politically Exposed Persons

A PEP is a natural person who is or has been entrusted with a prominent public function; close family members (spouse or legally recognised partner, children and their spouses, parents) and known close associates are treated as PEPs. PEP status is screened at account opening and re-screened on an ongoing basis. Where a customer is identified as a PEP:

- senior management approval (Compliance Officer or risk management officer) is required to establish or continue the relationship;
- the source of wealth and source of funds must be established; and
- enhanced ongoing monitoring is applied.

PEP and sanctions screening is run at account opening and thereafter on an ongoing basis across the existing player base. A positive or possible match is escalated immediately to the Compliance Officer, who decides whether to establish or continue the relationship and records the decision.

4.7 Sanctions screening

Compliance with sanctions imposed by the UN Security Council is mandatory under the SNO. The Company screens all players at registration and on an ongoing basis against the UN, EU and OFAC lists. A confirmed match results in immediate blocking of the account, no processing of any transaction, and escalation to the Compliance Officer for reporting.

4.8 Ongoing monitoring and re-verification

- Customer profiles are kept current so that unusual or suspicious activity can be identified against a known baseline.
- Customers are risk-classified on a scale of 1 to 6; a new customer is assigned a default risk level of 3.
- Risk level is recalculated on the basis of activity and activity patterns. A higher risk level increases the intensity and frequency of verification and may reduce bet, deposit and withdrawal limits.
- Risk mitigation may include bet amount limits, bet delay in seconds, restriction of payment methods, restriction from parts of the service (for example the casino section), or suspension of all transactions until EDD is complete.
- Where ML/FT activity is identified the matter is reported to the FIU as set out in Section 7.

4.9 Records

CDD and EDD records, transaction records, and records of the examination of the background and purpose of the relationship are retained for **at least five years after the end of the business relationship** or after the date of the occasional transaction. Records must be sufficient to permit reconstruction of individual transactions, including amounts and currency types, so as to provide evidence for prosecution if required. Data protection law does not override these retention obligations.

5. Player Account and Fund Management

License conditions Article 14(1)(b), Articles 6(5), 8 and 9. Source policies: Account, Pay-outs and Bonuses; Refund Policy; General Terms & Conditions.

5.1 One account per player

A player may open and use one account only. Where the Company has reasonable suspicion that a customer has opened or used multiple accounts, it may temporarily block or immediately close all such accounts. Winnings, bonuses, free bets and winnings accrued from those bonuses obtained through multiple accounts are void, and funds held in multiple accounts are withheld up to the amount covering any illegal withdrawals. A player who notices they hold more than one account is obliged to notify the Company immediately.

An account holder may not allow any other individual, including any minor, to use or reuse the account. All winnings obtained by allowing another individual to use the account are void.

5.2 Information available in the player account

Article 9(9) of the license conditions requires the Company to provide the player with access, at all times, to at least:

1. the current balance of the player account;
2. the opening balance at the most recent login;
3. the total stake since the most recent login;
4. total wins and total losses since the most recent login;
5. an overview of all transactions on the player account for at least the last 90 days;
6. the time within which prize money will be available after the end of the game; and
7. how long the prize money will remain available to the player — not less than 30 months from the date the prize money was awarded.

Separately, the CGA Responsible Gaming Policy requires the player to be able to access a detailed record of betting and wagering history, including transaction timestamps, for at least the last six months. Longer periods may be requested and must be provided within 10 working days.

5.3 Payment transactions

- All payment transactions between the Company and the player are carried out **exclusively through the player account** (Article 9(1)).
- The Company may appoint Payment Solution Providers to act, receive or pay funds on its behalf. Entering into a relationship with a payment processing supplier requires **prior CGA approval** (Article 2(6)).
- Where intermediaries are used for player transactions, the intermediaries must be registered and verified and all transactions recorded in an identifiable account. The CGA may require full disclosure of the intermediary agreement.
- Fiat currencies accepted as stakes must be tradable on regulated international markets; virtual currencies must be tradable on internationally licensed virtual currency exchanges.
- Currency exchange within or outside the player account is prohibited, as is exchanging virtual currency for fiat currency and offering investment alternatives to players.
- Prize money is paid out in the same currency, virtual or fiat, that was used to play the game.

The Company does not accept virtual currencies as stakes or bets. All deposits and withdrawals are made in fiat currency only.

Every payment method and payment service provider in use is recorded in the supplier register, together with the date of CGA approval where Article 2(6) applies.

5.4 Segregation of player funds and liquidity

All player funds — deposited, won, or otherwise owed to a player — are held in a **segregated account exclusively designated for that purpose** (Article 9(2)). Player funds are not used for operating expenses and are not commingled with corporate funds.

- The segregated player-funds balance is reconciled against the aggregate player liability recorded in the platform **daily**, with breaks investigated and cleared within one business day.
- A monthly reconciliation statement is signed off by the Head of Payments and reviewed by the Managing Director.
- Liquidity sufficient to pay out prize money is confirmed monthly and reported to the Board; any shortfall is treated as a material incident and escalated immediately.

The segregated player-funds account is held with Finductive Ltd. The account is designated exclusively for player funds and is reconciled and reported as set out above.

5.5 Withdrawals and payouts

1. When a game outcome is determined, or the result of an event is confirmed and markets are settled, winnings are credited to the player account.
2. Withdrawal requests are subject to completed CDD and, where risk requires it, EDD.
3. Additional verification is carried out for any payout, or payouts cumulatively exceeding the equivalent of **EUR 2,300**, and may be carried out at lower values. All transactions are checked to prevent money laundering.
4. Withdrawals are returned, wherever possible, to the payment source used for deposit.
5. Responsible gaming or AML measures may never be used as a pretext to delay a legitimate withdrawal.

The withdrawal processing time applicable to each payment method is published on the website and stated in the General Terms & Conditions, consistent with Article 12(1)(m).

5.5.1 Incorrect credits

Where the Company mistakenly credits an account with winnings or funds that do not belong to the player — through an error in published pay tables, gaming software or human error — the amount remains the property of the Company and is transferred out of the account. If a withdrawal has already completed using such funds, the amount constitutes a debt owed to the Company. Automated recovery may be attempted through the payment provider, and the player is obliged to notify the Company immediately. Bets accepted where the account had insufficient funds, or funded by mistakenly credited amounts, may be voided.

5.6 Refunds and chargebacks

Players must not request a chargeback directly from their bank or card provider. Refunds are granted only in reasonable and justified circumstances, and only where:

- the deposit method supports refunds;
- the request is made to support within a reasonable timeframe (24 hours);
- the balance and gaming activity are unchanged since the deposit — partial refunds are not supported and consumed balances must follow the withdrawal process;
- any bonus credits arising from the deposit are unconsumed, and are removed on execution of the refund.

Refunds are returned only to the original payment source; the refund route may not be used to move money between payment sources. The withdrawal process is always governed by enhanced due diligence. Where the origin of funds or the player's activity is contrary to the AML Policy, the Company may deny further deposits or withdrawals, freeze assets and return funds, and is obliged to inform the FIU.

5.7 Dormant accounts and inactivity

Where funds remain in an account with no activity for a prolonged period (over one year), the Company reserves the right to return the funds to the initial payment source where possible. Bonuses or points may expire after six months of account inactivity. The treatment of dormant accounts and balances must be set out in the General Terms & Conditions under Article 11(3)(i) of the license conditions.

5.8 Bonuses and promotions

- Offers are limited to one per person, family, household address, email address, telephone number, payment account, mobile device or shared device.
- Bonuses are available only to customers who have made a real-money deposit, and the first deposit bonus is not activated until KYC verification is complete.
- Bonus terms must be communicated transparently. Bonuses must not be used to encourage excessive gambling.
- Where a bonus term is breached, or a pattern of wagering produces guaranteed profit irrespective of outcome, the Company may reclaim the bonus element, settle bets at correct odds, void free bets, and levy an administration charge up to the value of the bonus.
- Bonus abuse — including breach of promotional terms and opening multiple accounts to claim multiple bonuses — may result in forfeiture of the bonus and its winnings, withdrawal of future offers, product access restriction, or account termination.
- **No bonus, free play or incentive may be offered to a player during a cooling-off period or to a self-excluded player.**
- **No credit may be offered to any player for the purpose of wagering.**

6. Responsible Gaming

License conditions Article 14(1)(c); CGA Responsible Gaming Policy v1.0 (17 April 2025). Source policies: Responsible Gaming; Self Exclusion; Gaming Addiction.

6.1 Responsible gaming function

The Company appoints a person to fulfil the Responsible Gaming role. Until a dedicated appointment is made, the Compliance Officer (not the AML/CFT Compliance Officer) is responsible for implementing and enforcing the Responsible Gaming policy. Whoever holds the role must provide a report to management **at least once every twelve months** on the effectiveness of the policy and related operational procedures, with recommendations for enhancement. **Any material change to the Responsible Gaming policy must be reported to the CGA**, and the policy must be uploaded to the CGA portal for evaluation.

The nine mandatory elements are: age verification; information accessibility; player self-assessment; behaviour tracking; cooling-off; self-exclusion; deposit limits; consumer advertising and marketing; and staff training.

6.2 Information accessibility

6.2.1 Responsible Gaming section

- A distinct Responsible Gaming section is available at all times, clearly identifiable and accessible.
- It contains easily understandable information enabling informed player choices.
- It gives direct access to every tool — self-exclusion, cooling-off, limit setting and other measures.
- It states how the player may contact the Company about responsible gaming concerns by email or chat.
- It is provided in English and in the language of the target market; the English version prevails in the event of discrepancy.

6.2.2 Homepage and Terms & Conditions

- A clear and visible link to the Responsible Gaming section appears on the website and app homepage.
- The Responsible Gaming section is explicitly referenced and included within the Terms & Conditions.
- The Terms & Conditions are no more than one click away from the homepage.
- Players are informed of the tools available, how they function, and how to use them.

6.2.3 Mandatory footer content

The footer of every page of www.goal365.bet must contain:

- a clear visual indication that under-age gambling is prohibited;
- the name and registered address of the license holder — Trigonon Group N.V., Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao;
- the official CGA license number — OGL/2024/659/0586;
- a statement confirming CGA regulatory oversight — "www.goal365.bet is operated by Trigonon Group N.V. and is licensed and supervised by the Curaçao Gaming Authority";
- a link to the Responsible Gaming section;
- the Company's CGA digital seal; and
- a direct link to one or more gambling addiction support resources (for example GamCare, Gamblers Anonymous, GambleAware), plus local support resources in the target market where available.

6.3 Player self-assessment

Players must be encouraged to assess their gambling habits through a self-assessment tool available in the Responsible Gaming section. The Company provides an on-site screening instrument — the CAGE questionnaire adapted for gambling, with a link to the Gamblers Anonymous 20-question test as an alternative (Cut down / Annoyed / Guilty / Eye-opener), with interpretation guidance: no "yes" answers indicates low risk; one indicates moderate risk; two or more indicates high risk and warrants further evaluation and intervention.

Any player who recognises problematic behaviour through self-assessment is directed to the available responsible gambling tools. Test results taken through third-party resources are not recorded by the Company.

6.4 Behaviour tracking and intervention

Article 1.4(e) of the LOK prohibits giving a person who can reasonably be assumed to be a vulnerable person the opportunity to play games of chance. The Company therefore monitors player behaviour holistically. No single indicator by itself classifies a player as at risk; a determination generally requires multiple indicators occurring simultaneously and consistently.

6.4.1 Key monitoring indicators

- sudden unexplained increases in deposit or wagering frequency, or in session patterns;
- repeated failed transactions due to insufficient funds;
- reversal or repeated cancellation of withdrawal requests;
- a pattern of inexplicably extended play sessions;
- unreasonably increased contact with customer support, including agitated requests for bonuses;
- frequent changes to responsible gaming tools — repeatedly setting or changing deposit or loss limits, or repeated use of cooling-off;
- indications of a player maxing out a credit card;
- attempts to open multiple accounts to bypass deposit or loss limits.

6.4.2 Detection method

Behaviour tracking is performed manually by trained frontline staff — customer support and VIP handlers — who are best placed to identify problematic behaviour through patterns and direct interaction. The Company does not currently use automated, AI or machine-learning detection tooling. The CGA permits frontline staff to be the primary detection method; where manual monitoring is relied on, the structured flagging process below and the training at Section 3.5 are the controls that make it effective.

A structured flagging process routes potential vulnerable players to the Responsible Gaming function for detailed behavioural analysis. Frontline staff review the indicators at 6.4.1 during every substantive player interaction and at least monthly across the active player base.

6.4.3 Profiling and escalation

1. Player profiles incorporating relevant data points are maintained to assess individual risk levels, and a risk-based approach determines the level of monitoring and intervention.
2. Every responsible gaming interaction — player-initiated or Company-initiated — is recorded in the Player Account Management system together with the indicators of concern and the actions taken.
3. A player exhibiting at-risk behaviour is informed of the tools available (deposit limits, cooling-off, self-exclusion).
4. Where a player exhibits behaviour reasonably suggesting vulnerability, the Company initiates direct contact advising the player to review the Responsible Gaming section and consider the tools and support services.
5. Escalation may include applying mandatory deposit limits, temporarily suspending the account pending assessment, or permanently excluding the player in cases of severe or persistent risk.

6.5 Cooling-off

Parameter	Requirement
Duration options	24 hours, 7 days, 1 month, 3 months
Wagering	Blocked — all activity, or by vertical if the operator offers that option
Deposits	Blocked
Withdrawals	Permitted — player funds remain accessible
Log-in	Permitted; account remains active with gambling features disabled
Brand scope	Current brand (including mirror domains) or all Company brands, at the player's selection
Marketing	Opt-out offered; if opted out, no marketing may be sent. No bonuses, free play or incentives during the period
Ante-post bets	Remain in place
Active poker tournaments	Must be completed
Changes during the period	May be made more restrictive only
Activation	Self-executed by the player online. In exceptional cases by email or chat, with the elected options enabled within 24 hours
Reactivation	Automatic on expiry — no further action required by the player

Duration and marketing opt-out are mandatory categories; brand and vertical options are at the Company's discretion. The player selects preferences by tick-box; tick-boxes must not be pre-checked. Restrictions take effect immediately.

The Company must not question the player's decision, offer bonuses or promotions to encourage continued play, or delay or complicate activation. A single neutral online confirmation is permitted for the 1-month and 3-month options, for example: "You wish to cool off for one month. Please confirm."

6.6 Self-exclusion

Parameter	Requirement
Duration options	1 year, 3 years, 5 years, 10 years, lifetime (minimum 1 year under LOK clause 5.4(2))
Wagering	Blocked — all verticals
Deposits	Blocked
Withdrawals	Depends on civil law
Log-in	Blocked — the account is closed
Brand scope	All brands and domains under the Company's license — automatic
Marketing	Automatic opt-out; all messages blocked
Ante-post bets	Voided and refunded, subject to AML/CFT regulations
Active poker tournaments	Must be completed
Progressive jackpot contributions	Contributions made before the request remain in situ; the player is no longer entitled to participate in the jackpot
Changes during the period	None — irrevocable and irreversible for the duration selected
Activation	Player must be able to initiate and complete the process fully online, without email or operator approval. In exceptional cases by email or chat, enabled within 24 hours
Reactivation	Only after the period ends, and only on the player's written request by email or chat. The Company may not initiate reactivation contact

The player selects the duration by tick-box; all other elements are automatic. Restrictions take effect immediately. Any wagering taking place after the request and before it takes effect must be voided and funds returned to the player, subject to civil law. The Company must have robust measures to identify duplicate accounts where reasonably possible and to prevent self-excluded individuals from creating new accounts under different credentials. Where possible, and in line with applicable regulation, any payment method known to the Company and used by a self-excluded player is blocked for future use during the exclusion period.

6.7 Operator-initiated exclusion

The Company may exclude a player as a high-risk intervention measure where the player displays problematic gambling behaviour, or attempts or engages in criminal activity through the platform. The Company **may not** exclude players solely on the basis of the amount of their winnings. Operator-initiated exclusions are formally documented and records are kept for **at least five years**; the CGA may request these records at any time.

6.8 Deposit limits

- Players may set deposit limits for daily, weekly or monthly periods.
- Once a limit is reached, no further deposits are possible until the period resets.
- A request to increase the severity of a limit (a lower limit) takes effect immediately. A request to decrease the severity of a limit (a higher limit, or removal) is subject to a 24-hour waiting period.
- Resolved or unresolved wagers placed before a limit was set are unaffected.
- Limits always apply against the current time — a daily limit reached at 23:59 prevents further deposits until the same time the following day.

6.9 Other limits and reality check

In line with the target market and player profile the Company may offer loss limits, time limits and wager limits. Bet limits are offered: a decrease takes effect immediately and an increase is subject to a 24-hour waiting period.

Reality Check measures, where used, must be fit for purpose and may include a real-time session timer visible while logged in, a real-time clock in the player's time zone, periodic pop-up reminders about session duration, and player-activated reality

checks at customised intervals. A customised reality check must suspend play momentarily and require the player to confirm they have read the message before resuming, and should indicate how long the player has been playing and their winnings and losses in that period.

6.9.1 Exceptions affecting active wagering

Where a limit or exclusion would affect active gameplay — a time limit set during a poker tournament, or an unresolved ante-post bet — the restriction is honoured immediately with the exception of the active gameplay or wager. No further wagering is permitted before completion: a player may not enter another tournament while one is in progress, nor place further wagers while an ante-post bet remains unresolved.

6.10 Internet filtering

The Company reminds adults to safeguard usernames, passwords and payment details when sharing devices with minors, and provides links to third-party blocking software such as BetBlocker, GamBlock and Gamban.

6.11 Advertising and marketing

The Company must not engage in irresponsible advertising. The following are prohibited:

- targeting vulnerable people, including through visual content;
- portraying gambling as a way to achieve financial success or solve financial difficulty;
- suggesting that skill can influence the outcome of games based purely on chance;
- portraying gambling as a substitute for financial, emotional or mental well-being;
- featuring minors or depicting them engaging with gambling content;
- overt sexual or pornographic imagery or suggestion;
- linking gambling to smoking, drug use, alcohol consumption, seduction or enhanced attractiveness.

A clearly visible responsible gaming message or slogan must appear on all advertising.

The Company does not engage affiliates, social media influencers, brand ambassadors or sponsorship partners. All marketing is produced and published by the Company itself. Should the Company engage any such third party in future, it will remain responsible for the wording and visual representation of any paid placement or advertisement, will make that party aware of the Responsible Gaming policy, will require adherence to it, and will notify the CGA where the arrangement constitutes a critical change.

7. AML / CFT / CPF

License conditions Article 14(1)(e); NORUT; NOIS; SNO; CGA Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation (January 2025). Source policy: Anti-Money Laundering Policy.

7.1 Objective

Money laundering is the process of making funds originating from criminal activity appear to originate from a legitimate source; terrorist financing is the use of funds to finance terrorism. Because the Company's services are widely used and transacted remotely, they may be targeted by criminals seeking to launder money through online betting and casino play. The Company is obliged by law to combat both, and to combat the financing of proliferation of weapons of mass destruction.

7.2 AML compliance programme

The programme comprises the five elements required by the CGA AML/CFT/CPF Regulations:

1. A system of internal policies, procedures and controls — this Manual, the AML Policy and the supporting work instructions.
2. The appointment of a Compliance Officer meeting the CGA requirements set out at Section 3.3.
3. An employee screening programme and an ongoing employee training programme.
4. An independent audit function to test the AML programme.
5. Cooperation with examination by the CGA.

7.3 Risk-based approach

7.3.1 Business Risk Assessment

The Company documents a Business Risk Assessment covering customer, product/service, delivery-channel/interface, geographic and technological risk. The Company's standing assessment is:

Risk factor	Position	Rating
Customers	Non-face-to-face, remote registration and transaction	HIGH (6–8/10)
Service / product	Web-based betting and casino platform	HIGH (6–8/10)
Interface	Internet-only connection between the Company and its customers	HIGH (6–8/10)
Geography	Operation across several jurisdictions subject to respective licenses	HIGH (6–8/10)
Payments	No cash accepted; all payments routed through verified and regulated providers that themselves apply CDD/EDD	Mitigating — but not relied on in isolation

Because customers are not face-to-face, risk is by default high and EDD applies to all customers. The Business Risk Assessment is reviewed at least annually and after any material change in product, market, payment method or technology, including the introduction of new technologies such as virtual currency acceptance or AI-driven tooling.

7.3.2 Customer Risk Assessment

Customers are risk-classified on a 1–6 scale, with a default of 3 on account opening. All customers undergo CDD and EDD; the risk level determines the frequency and intensity of verification and the limits applied. The risk level is recalculated on the basis of activity and activity patterns. Risk mitigation measures available are set out at Section 4.8.

The Business Risk Assessment and the Customer Risk Assessment methodology are maintained by the Compliance Officer as separate documents, are reviewed at least annually, and are produced to the CGA and to independent experts on request.

7.4 Customer due diligence

CDD, EDD, PEP and sanctions screening are described in full at Section 4. The AML-specific timing rule is repeated here: minimum identification data (name, permanent residential address, date of birth) plus PEP and sanctions screening are collected and run **at account opening**; full CDD measures must be complete by the time cumulative deposits and withdrawals reach **NAf. 4,000**, calculated daily since the start of the relationship and including peer-to-peer transfers. Linked transactions individually below the threshold but cumulatively meeting or exceeding it are treated as reaching the threshold.

7.5 Transaction monitoring

Transactions are monitored on an ongoing basis against the customer's known profile and the indicators set out in the Regulation Indicators Unusual Transactions. Monitoring covers deposits, withdrawals, transfers, gameplay patterns, and payment-method changes, including credit card and e-wallet transactions.

- Automated alerts are generated against configured rules and thresholds.
- Alerts are triaged by first-line staff and escalated to the Compliance Officer where an indicator is met.
- Monitoring outputs are reviewed by the Compliance Officer, and controls are updated where the risk picture changes.
- Audits are performed to review risk management, mitigation strategies and employee compliance.

The monitoring rule set — alert types, thresholds, triage service levels and the escalation route — is maintained by the Compliance Officer as a separate working document and is reviewed at least annually.

7.6 Internal and external reporting

7.6.1 Internal reporting

All unusual individual transactions or series of transactions listed in the Regulation Indicators Unusual Transactions must be reported internally **without any delay**, with supporting documents. Every member of staff has a duty to report a knowledge or suspicion of ML/FT through the designated internal channel to the Compliance Officer. Procedures for internal and external reporting are communicated to all personnel.

7.6.2 External reporting to the FIU

- The Compliance Officer prepares the external report of unusual transactions and files it with the FIU **without delay**, in English, together with all supporting documents, through the reporting channel required by the FIU.
- The Company, its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure when reporting to the FIU.
- The Company responds promptly to any request for information from the FIU, and in any event within five working days.

7.6.3 Prohibition of disclosure (tipping-off)

The Company, its senior management and its employees must not disclose any detail or information in connection with a report filed to the FIU, or a request for information made by the FIU, to the customer or to any third party. Caution is required when terminating a relationship or blocking transactions following a report, since drastic action may alert the player. Where possible the preferred response is to increase ongoing monitoring and submit further reports rather than to take action that risks tipping off.

7.6.4 Blocking and freezing

The Compliance Officer maintains an internal procedure defining when the reporting of an unusual transaction leads to blocking or freezing of a player account, balancing the ML/FT risk against the tipping-off prohibition. Any freeze is documented with the decision-maker, the rationale and the date.

7.7 Employee screening and training

Proportionate background screening is applied to critical or sensitive roles, subject to applicable law, and confidentiality obligations are imposed on all staff and contractors. AML/CFT training is delivered on appointment and at least annually, is documented, and is tested; employee compliance is checked periodically. The Compliance Officer supervises the AML training programme.

7.8 Independent audit

An independent audit function tests the AML programme. Testing includes, at minimum, a sampling of unusual transactions at and beyond the applicable thresholds followed by a review of the decisions taken, verification of CDD file completeness, review of training records, and assessment of the adequacy of the risk assessments. Findings are assigned an owner and a target date and are reported to the Board.

The independent audit is performed by a party independent of the first and second lines. Findings, owners and target dates are recorded in a remediation tracker held by the Compliance Officer and reported to the Board.

7.9 Records

All necessary records on transactions, both domestic and international, are retained for **at least five years**, and must be sufficient to permit reconstruction of individual transactions including amounts and currency types. All records obtained through CDD measures, account files and business correspondence are retained for at least five years after the business relationship ends or after the date of an occasional transaction. Records of internally and externally reported unusual

transactions are maintained by the Compliance Officer. CDD information and transaction records are made available to domestic competent authorities on appropriate legal authority.

8. Information Security

License conditions Article 14(1)(d) and Articles 6, 7 and 13(6); CGA Information Security Control Requirements — CIS Controls Implementation Group 1. Source policy: Trigonon Group N.V. Information Security Policy v1.0.

8.1 Relationship to the Information Security Policy

The Company maintains a standalone Information Security Policy that adopts the CGA Information Security Control Requirements and CIS Controls Implementation Group 1 as its security baseline. That policy is the controlling document; this section summarises the operational commitments most relevant to the licensed operation. Where a CGA requirement, license condition or Curaçao law imposes a higher or more specific obligation, that obligation prevails.

8.2 Governance of security

- The Board retains accountability and designates a member of Senior Management to coordinate the policy, report material risks and oversee remediation. Consistent with the proportionate CIS IG1 baseline, a dedicated Information Security Officer is not appointed.
- Technical tasks may be performed by qualified employees, the platform provider, the cloud provider or a managed security provider; outsourcing does not remove regulatory accountability.
- A control-responsibility matrix records, for each applicable control, the responsible party and the supporting evidence.
- An information-security risk assessment is documented at least annually and after any material change or serious incident.
- Exceptions require documented risk justification, approval by the Policy Owner, compensating controls and an expiry or review date.

8.3 Control summary

Control area	Operational commitment
Assets and software	Inventories of hardware, network devices, software and gaming components reviewed at least twice yearly; weekly process to detect unauthorised devices; monthly check of software support status.
Data protection	Data classified as Critical Gaming Data, Player Personal Data, Business Confidential or Public; register of storage, processing, transmission and backup locations; least privilege; encryption in transit and at rest; defined retention and secure disposal; masking of player data in development and test.
Secure configuration	Documented secure baselines; unnecessary services and ports disabled; default accounts and credentials removed or changed before production; host and network firewalls with authorised, recorded rule changes; encrypted administrative protocols (SSH, SFTP, HTTPS).
Accounts and access	Inventory of user, administrator and service accounts reviewed at least quarterly; role-based access with recorded approval; immediate revocation on termination; separate administrator accounts; MFA on all externally accessible applications, remote access and administrative access; passwords at least 8 characters with MFA and at least 14 without.
Vulnerability and patch	Documented risk-based vulnerability process; vulnerability scans at least monthly; OS, application, firmware and network patching at least monthly with recorded approvals and exceptions.
Logging and monitoring	Audit logging on endpoints, servers, applications and security tools; critical logs to central, access-restricted, tamper-resistant storage; time synchronisation; critical gaming logs covering player activity, gameplay and betting transactions, game outcomes, jackpot and high-value events, deposits, withdrawals, bonuses, adjustments, administrative access and configuration changes.
Malware, web and email	Supported and updated browsers and email clients; DNS or equivalent web filtering; centrally managed automatically updated anti-malware; removable media authorised, scanned and auto-execution disabled.
Backup and continuity	Documented recovery process with RPO and RTO; automated backups at least weekly and more frequently for high-volume gaming and financial transaction data; encrypted backups with offline, off-site or immutable storage; restoration testing recorded; business continuity and disaster recovery tested at least annually.

Control area	Operational commitment
Third parties and gaming integrity	Current provider inventory; proportionate security due diligence before onboarding and periodic monitoring; contractual confidentiality, security, incident notification and audit rights; verification of game, RNG and platform certifications at onboarding and at least annually; authenticated and encrypted sports and gaming feeds with integrity validation and market suspension where integrity cannot be assured.
Personnel and physical	Security awareness training on appointment and at least annually; confidentiality obligations and proportionate background screening; asset recovery and access removal on termination; restricted physical access to offices and server rooms; clean-desk and clear-screen practices.

8.4 Availability and continuity of service

Article 6(2) of the license conditions requires that games are available to players at all times in a secure manner and without interruption of service. The Company maintains appropriate failover or redundancy for mission-critical services, tests business continuity and disaster recovery at least annually and after significant change, and treats an unplanned outage of the gambling interface as a reportable incident where it may affect regulatory reporting, system availability or game fairness.

8.5 Security incidents and CGA notification

- A documented incident-response procedure is maintained, with a primary and backup incident coordinator, current internal and external contacts, escalation criteria, reporting templates and evidence-preservation requirements.
- Employees and providers must report suspected incidents immediately through the designated internal channel.
- The Company notifies the CGA **without undue delay and in any event within 24 hours** of a security incident that compromises gaming integrity, affects player funds or personal data, or may impact regulatory reporting, system availability or game fairness.
- Other authorities and affected persons are notified where required by applicable law, including under the National Ordinance on the Protection of Personal Data.
- Material incidents receive a documented post-incident review and corrective actions.

The full incident and change reporting regime, including the 24-hour clock, is set out at Section 14.

8.6 CGA data access

Article 13(6) requires that critical information concerning players, their game transactions and their financial transactions remains accessible to the CGA through a server hosted in a Tier-IV certified data center. The Company provides requested information, permits authorised assessments and inspections, and cooperates with CGA oversight, including remote scanning and automated compliance verification where lawfully deployed.

The Company's gaming platform and player data are hosted on Amazon Web Services (AWS).

8.7 Assurance

- An annual self-assessment is completed against all applicable CGA IG1 controls using the required form or current CGA instructions.
- Independent third-party security audits are arranged where required, with findings, remediation owners and target dates maintained.
- An applicable-obligations register covers gaming, information security, privacy, AML/CFT/CPF and relevant contractual requirements.
- Evidence of control operation is retained — inventories, approvals, reviews, scan and patch results, logs, backup tests, training, supplier checks, incidents and remediation.

9. Suspension and Closure of Player Accounts

License conditions Article 14(1)(f).

9.1 Grounds

Ground	Typical action	Owner
Player is, or is found to be, a minor	Immediate closure; bets void; deposits reimbursed; winnings forfeited; reason communicated to the player	KYC / Compliance
Self-exclusion requested by the player	Account closed for the selected duration; no log-in; marketing blocked	Responsible Gaming
Cooling-off requested by the player	Gambling features disabled; account remains active; withdrawals permitted	Responsible Gaming
Operator-initiated responsible gaming exclusion	Documented exclusion following escalation; records kept 5 years	Responsible Gaming
CDD/EDD not completed within 30 days of the Naf. 4,000 threshold	Relationship terminated; FIU report if presumption of ML/FT; otherwise funds returned to source	AML Compliance
Sanctions list match	Immediate block; no transactions processed; escalate to Compliance Officer	AML Compliance
Suspected ML/FT	Internal report; blocking or freezing per internal procedure, weighed against tipping-off risk	AML Compliance
Multiple accounts / account sharing	Temporary block or closure of all accounts; winnings and bonuses from those accounts void; funds withheld up to illegal withdrawals	Fraud / Compliance
Bonus abuse	Bonus and bonus winnings forfeited; product restriction; exclusion from future offers; account termination in serious cases	Fraud / Compliance
False or misleading registration information	Account blocked or closed following verification failure	KYC
Player request to close	Closure; full balance paid out unless fraudulent behaviour is suspected	Customer Support
Company-initiated closure	Permitted under the General Terms & Conditions; full balance paid out unless fraud is suspected; contractual obligations to the player must first be fulfilled	Management

9.2 Procedure

1. The trigger is recorded in the Player Account Management system with the ground, the evidence and the decision-maker.
2. The account status is changed on the platform, and the effect on log-in, play, deposit and withdrawal is set according to the ground.
3. Open positions are handled: active poker tournaments must be completed; ante-post bets remain in place for cooling-off and are voided and refunded for self-exclusion, subject to AML/CFT regulation.
4. The player is notified in writing of the action and the reason, except where notification would constitute tipping-off in an ML/FT context.
5. Balance treatment is determined and executed, subject to completed CDD and any AML restriction.
6. The record is retained for at least five years and is producible to the CGA on request.

9.3 Reinstatement

- A cooling-off account reactivates automatically on expiry, with no player action required.
- A self-excluded account may be reinstated only after the selected period has ended and only on the player's written request by email or chat. The Company may not initiate reactivation contact. Reactivation may be prompted at the point the player attempts to log in after the period has ended.

- An account closed for a compliance ground is reinstated only with the documented approval of the Compliance Officer.
- An account closed because the holder was a minor is never reinstated for that individual before the age of 18, and only after full re-verification.

10. Games, Gaming Equipment and Software Integrity

License conditions Articles 7 and 10. Source policy: Fairness & RNG Testing Methods.

10.1 Certification

- All remote games of chance owned by the Company must be **certified for soundness and integrity by a testing laboratory approved by the CGA**.
- The Company must ensure that all games supplied by third-party providers and offered to players are certified by a CGA-approved testing laboratory.
- Third-party game suppliers must be disclosed on the CGA online gaming portal.
- Gaming equipment and application software must comply with international standards and be tested for information security and integrity by an independent qualified entity approved by the CGA.

Each game provider is reviewed and tested against the specifications it supplies before integration. Test documentation must carry a unique test number and be issued by the official authority; the provider must attach specifications, testing results and any game licenses. Where a random number generator device is used, its specifications and license are obtained and reviewed before any further business is transacted.

A certification register is maintained recording, for each provider and game or module, the CGA-approved testing laboratory, the certificate number, the issue and expiry dates and the current status. The register is produced to the CGA on request.

10.2 Ongoing integrity monitoring

- Game statistics are examined periodically against specification, on the Company's own initiative and without needing to be prompted by a player. Where a game does not meet specification over the long run, a report is issued to the provider; depending on the outcome the game may be removed from play or the provider banned.
- Game versions are kept up to date so that players use the latest version with current features and security patches.
- Any problem reported by a player relating to a game is forwarded to the provider, with further action determined by severity.
- A game found not to meet standards, through a bug or otherwise, is removed from play and reactivated only on proof that the issue is resolved.
- Certification lapses or withdrawals are escalated, the affected content is suspended and the CGA is notified where required.

10.3 Inventory and maintenance

Article 7(3) requires an up-to-date inventory of gaming equipment, the gambling interface (both physical and virtual), the application software and the games offered. The CGA may request an updated inventory at any time. The Company is responsible for regular maintenance and for replacing or expanding equipment and software as necessary to ensure the integrity of the operation.

The inventory is maintained by the NOGC Compliance Officer, reviewed at least twice each year, and produced to the CGA on request.

10.4 Sports data and market integrity

Sports and gaming feeds are authenticated and encrypted, integrity validation is applied, and availability and anomalies are monitored. Where feed integrity cannot be assured, affected markets or content are suspended. Suspected match-fixing or manipulation is escalated to the Compliance Officer and reported to the CGA as an incident and, where applicable, to the relevant sporting body and law enforcement.

10.5 Change management

Changes to the gambling interface, application software, game portfolio or platform configuration are recorded, risk-assessed, tested and approved before release, with rollback steps defined. Changes that constitute a critical change under Article 4 — including the addition or removal of domains, or entering into a relationship with a platform, game content or payment supplier — require **prior CGA permission** before implementation.

11. Suppliers and Outsourcing

License conditions Articles 2(6), 3(2) and 4.

11.1 Prior CGA approval

The Company must obtain prior approval from the CGA before entering into a relationship with a supplier providing goods or services related to:

1. the development, operation or maintenance of gaming platforms;
2. the provision of games or gaming content; and
3. the handling of payment processing or financial transactions.

Entering into such a relationship without prior permission is a critical change breach under Article 4.

11.2 Supplier lifecycle

Stage	Requirement
Pre-selection	Confirm the supplier category requires CGA approval; submit the request through the CGA portal and obtain permission before contracting.
Due diligence	Proportionate security, integrity and financial due diligence; verification of game, RNG and platform certifications; ownership and sanctions screening of the supplier.
Contract	Confidentiality, security obligations, incident notification, data protection, right to audit or request evidence, service levels, exit and data-return provisions.
Register	Maintain a current inventory of providers, services, data exchanged, security responsibility, certification or audit status and contractual controls.
Monitoring	Periodic review of performance, certification validity (at least annually for CGA-regulated B2B game providers) and security assurance evidence such as recognised audit or certification reports.
Exit	Documented offboarding: access revocation, data return or secure deletion, and notification to the CGA where the change is critical.

The supplier register records the platform, game content, live casino, sports data, payment, KYC and hosting providers in use. Hosting is provided by Amazon Web Services (AWS) and player funds are held with Finductive Ltd. For each supplier falling within Article 2(6), the register records the date on which CGA approval was obtained.

12. Player-Facing Transparency

License conditions Articles 11 and 12.

12.1 General Terms & Conditions — mandatory content

The general terms and conditions must be available to the player at all times, unambiguous, and written clearly in English and, where the target market's language is not English, in that language. They must contain at least provisions on:

#	Required provision	Content published by the Company
a	Amendment of the general terms and conditions	Included
b	Name, business address and Chamber of Commerce number of the license holder	Trigonon Group N.V., Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao, Chamber of Commerce No. 142028
c	Obligations of the player before opening a player account	Included
d	Conditions under which a player account is closed or access suspended	Included
e	Conditions under which distribution of player funds and winnings may be suspended, cancelled or declared invalid	Included
f	Rules on the currency used for stakes and prize money	Stakes are accepted only in fiat currencies tradable on regulated international markets; no currency exchange is performed in or outside the player account; prize money is paid in the same currency used to play
g	Retention period of all communications relating to participation in games	All communications relating to participation in games are retained for five years
h	Responsible gaming policy, including deposit limits and self-exclusion	Included
i	Player withdrawal requests and handling of dormant accounts and balances	The withdrawal request process is stated; where an account shows no activity for over one year the Company may return the balance to the original payment source; bonuses or points may expire after six months of inactivity
j	Applicability of Curaçao law and jurisdiction of the Curaçao court	Governed by the laws of Curaçao; the parties submit to the jurisdiction of the Curaçao courts and to the rules of arbitration of the Curaçao Arbitration Centre
k	Complaints procedure and ADR under Article 5.3 LOK	Included

Players must be able to review changes to the terms in a sufficiently clear manner to decide whether to continue playing. The terms must be consultable at all times via the publicly accessible part of the gambling interface, reachable from any page.

12.2 Publicly accessible information

The following must be correct, up to date and available on the publicly accessible part of the gaming interface, in English and in the target-market language:

#	Required information	Content published by the Company
a	Name and trade name registered with the Chamber of Commerce	Trigonon Group N.V.
b	Chamber of Commerce registration number	142028
c	Date the license was issued and its duration	License OGL/2024/659/0586, granted 23 May 2025

#	Required information	Content published by the Company
d	Geographic address, contact details and customer service contact details	Kaya Richard J. Beaujon Z/N, P.O. Box 6248, Willemstad, Curaçao; support@goal365.bet and live chat
e	Statement that the CGA is the licensing authority and supervisor	"www.goal365.bet is operated by Trigonon Group N.V. and is licensed and supervised by the Curaçao Gaming Authority"
f	Reference to the general terms and conditions	Link to the General Terms & Conditions, reachable from every page
g	Prohibition of participation by minors or other vulnerable persons	Participation by minors and by other vulnerable persons is prohibited
h	Games offered, game rules, odds of winning, method of determining odds and, so far as possible, payout percentage	Game rules and the theoretical return to player are published per game or per provider, drawn from the certification documentation held under Section 10.1
i	Total costs associated with participating	Any deposit, withdrawal or currency-conversion charge borne by the player is stated
j	Specific costs for use of the technology of the games offered	Any charge for use of the gaming technology is stated
k	Information about gambling addiction and where to seek help	Gambling addiction information and links to support organisations
l	Complaints and disputes procedure	Complaints and dispute resolution policy, including ADR
m	Period within which prize money is made available after the end of the game	The crediting time after settlement and the withdrawal processing time by payment method
n	Currency in which prize money is payable	Prize money is payable in the same currency, fiat or virtual, that was used to play the game
o	How players can limit their stakes or participation	Deposit limits, bet limits and cooling-off
p	How a player can exclude himself from participation, registration and marketing	Self-exclusion and marketing opt-out
q	Other elements of the responsible gaming policy	Responsible Gaming section
r	CGA digital seal displayed at all times	The CGA digital seal, linking to the Company certificate at cert.cga.cw

The Company informs players in a timely manner of changes to this information, drawing attention to the changes on login.

13. Complaints, Disputes and ADR

License conditions Articles 11(3)(k) and 13; Article 5.3 LOK; CGA Player Complaints Policy Guidelines v1.1. Source policy: Player Complaints and Dispute Resolution Policy.

13.1 Definitions

Term	Meaning
Player interaction	Any written communication initiated by a player to customer service — general enquiries, feedback, or requests for information, assistance or clarification.
Complaint	A written expression of dissatisfaction relating to the Company's services, decisions, terms or conduct, indicating the player is unhappy and expects a response or resolution. For reporting purposes, a complaint is one where a Complaint Submission Form has been submitted and/or the matter has been escalated to ADR.
Dispute	A complaint not resolved to the player's satisfaction through the internal process and escalated, either internally or to an independent third party (ADR provider or court).

13.2 Submission

- Complaints may be lodged **free of charge at any time up to six months** after settlement of the bet or the incident complained of. For P2P (such as poker) and ante-post fixed-odds betting, the six-month clock runs from bet settlement or the conclusion of the event, not from placement.
- For in-running sports betting, players are advised that although they may complain within six months, prompt action may be necessary because data specific to the complaint may no longer be available after a short period.
- Only the registered player may complain. Under Article 1.3(c) LOK a player may not sell, donate, rent, lease, pawn or pledge any claim against a CGA license holder.
- Customer support is offered by email (support@goal365.bet) and live chat.
- An official **Complaint Submission Form** is available — downloadable for completion and email or upload, and/or fully completed and submitted online — in English and in the language of the website the player is using.

The form must capture, at minimum: complainant's name, address and place of residence; account number if applicable; date of the complaint and date of the disputed event; and a description of the conduct disputed, using predetermined category topics where applicable. Supporting documentation may be requested where reasonable in the context of resolution.

13.3 Resolution timelines

Complaint type	Acknowledgement	Resolution	Extension
Responsible gaming complaints	Within 2 days, in writing, with an explanation of the process and the average resolution timeline	Best efforts within 5 business days	Up to 2 weeks with notice to the player; a further 2 weeks if the delay is caused by a slow or absent player response
All other complaints	Within 7 days (1 week), in writing, with an explanation of the process and the average resolution timeline	Within 4 weeks	Once, by a further 4 weeks, with prior written notice

A complaint is categorised as responsible gaming whenever it concerns the targeting of vulnerable players, or the availability or timely implementation of self-exclusion or cooling-off and the consequences mandated in the Responsible Gaming policy. These are prioritised because of the potential impact on player well-being.

13.4 Outcome

The player always receives a final determination in writing, being either a reasoned final assessment of the outcome with supporting evidence where necessary, or detailed reasons for not handling the complaint. Where additional information is reasonably required, it must have been requested within the initial four-week period; if the player does not provide it within that period the complaint may be rejected. If the player remains dissatisfied and says so, the player is informed of the right to escalate to an independent ADR entity.

13.5 Use of artificial intelligence

- AI may assist with initial triage and acknowledgement of complaints.
- Once a complaint is identified as relating to responsible gaming, communications with the player must be conducted by a human, not AI.
- Complaints that can reasonably be considered complex, or that involve potential regulatory breaches, must be handled by a human.
- AI records are monitored to ensure recommendations and outcomes are reasonable, fair and consistent across like-for-like complaints.
- A player may request at any time that the complaint be handled exclusively by a human representative.

13.6 Alternative Dispute Resolution

- The Company must offer independent ADR services free of charge to players; **the Company bears all costs of the ADR process.**
- An agreement with at least one CGA-certified ADR entity must be uploaded to the CGA portal within one month of publication of the certified ADR providers on the official website.
- Full details of the ADR process must be included in the General Terms & Conditions, together with contact information for the ADR provider.
- Once an ADR process is completed it cannot be recommenced by either party with a different ADR entity. Where a player withdraws after the process has begun, the dispute cannot be resurfaced.
- Except where mutually agreed under the specific ADR terms, the Company must not restrict the player's right to take legal action.
- Where the Company sets ADR parameters to prevent abuse — such as a minimum claim value, whether ADR must precede legal proceedings, or the binding nature of the outcome — it should take independent legal advice. The CGA assesses each case on its merits; a claim concerning the admission of a self-excluded person is expected to be taken seriously regardless of monetary value.

13.7 Role of the CGA

The Company must make the role of the CGA clear to the player in the General Terms & Conditions. The CGA does not resolve or decide individual player complaints regarding gambling-related transactions, and will not review or overturn decisions of the Company or the ADR provider unless a matter is deemed to have been inadequately handled. The Company must not restrict the player's ability to contact the CGA directly on matters including malpractice, breach of license conditions or whistleblowing. Contact: complaints@gamingcontrolcuracao.org.

13.8 Records and reporting

- Reports are submitted to the CGA each year, covering complaints submitted through the Complaint Submission Form since the previous reporting period.
- Each report summarises: total complaints made; total settled (upheld and rejected); pending or unresolved; number by category; number referred to ADR; and the number and detail of complaints where the player has taken legal action.
- Records of unresolved complaints and of complaints escalated to ADR or legal proceedings are kept for the lesser of five years or the period stipulated by data protection, limitation or other applicable law.
- The CGA may request access to complaint and pending dispute records at any time.

13.9 Visibility

The complaints procedure statement is visible and accessible on the website as a standalone link or document, and is also clearly outlined in the General Terms & Conditions, including links to customer service, the information required to make a complaint, links to the online and downloadable forms, timelines, the player's rights including ADR and regulatory escalation, an explanation of the consequences of the ADR decision on further legal recourse, ADR contact details, and a clear statement that the CGA does not mediate individual disputes.

14. Regulatory Reporting and CGA Interaction

License conditions Articles 4 and 13.

14.1 Reporting obligations

Report	Trigger / frequency	Owner
Change report	On any change required to be notified under the NOGC and CGA instructions	NOGC Compliance Officer
Incident report	Within 24 hours of the incident, via the CGA portal	NOGC Compliance Officer
Player transaction report	Per Article 5.10 NOGC and CGA instructions	Head of Payments / Compliance
Complaints report	Each year	Head of Customer Support / Compliance
ADR report	Per CGA instructions; ADR providers also report separately under the ADR policy	Compliance
NORUT/NOIS independent expert report	Periodically, on CGA request, by an independent expert approved by the CGA	AML Compliance Officer
System design and responsible gambling independent expert report	Periodically, on CGA request, by an independent expert approved by the CGA	NOGC Compliance Officer
Responsible Gaming effectiveness report	At least every 12 months, to management; material policy changes reported to the CGA	Responsible Gaming Officer
CIS IG1 information security self-assessment	Annually, on the required CGA form	Information Security lead
Unusual transaction report	Without delay, to the FIU	Compliance Officer

14.2 The 24-hour incident clock

Under Article 5.10(6) NOGC the incident report must be submitted within 24 hours of the incident. Where reasonable assessment requires further investigation to determine whether an incident has occurred, the 24-hour period begins at the moment the investigation confirms it. **For change reports and incident reports the 24-hour period always runs from the moment the incident occurs.**

Reportable incidents include, without limitation: a security incident compromising gaming integrity, player funds or personal data; a material unplanned outage of the gambling interface; a game or RNG certification lapse or withdrawal; suspected match-fixing or feed manipulation; a material failure of player fund segregation or liquidity; a data breach; and a material failure of a responsible gaming control such as the admission of a self-excluded player.

The 24/7 incident contact for the licensed operation is +357 96538375. The Compliance Officer is the primary incident coordinator and files the CGA incident report. A weekend or holiday incident runs against the same 24-hour clock.

14.3 Critical changes requiring prior CGA permission

Under Article 4 it is not permitted, without prior CGA permission, to:

- change or add one or more ultimate beneficial owners, holders of a qualifying interest, directors or other key persons;
- remove, change or add domains;
- enter into a relationship with a supplier as referred to in Article 2(7) NOGC (platform, game content, payment processing);
- amend the articles of association of the license holder; or
- make any other change, amendment or addition determined by the CGA in accordance with the NOGC.

A change-control log records each proposed critical change, the date the CGA request was submitted, the date permission was received, and the date of implementation. **Implementation before permission is a license breach.**

14.4 Portal and checklist

The Company maintains its CGA online gaming portal account, keeps the domain list current, discloses third-party game suppliers, and completes the action points in the portal checklist within the time limits stated. The checklist forms an integral part of the license.

The Company's CGA online gaming portal account is administered by EGIS – FZCO, which also acts as the Company's ADR provider. The NOGC Compliance Officer remains accountable for the accuracy and timeliness of everything submitted through the portal.

15. Business Continuity, Wind-Down and Records

15.1 Business continuity

The Company maintains and tests business continuity and disaster recovery arrangements at least annually and after significant change, including appropriate failover or redundancy for mission-critical services, defined recovery point and recovery time objectives, and recorded restoration testing.

Recovery point and recovery time objectives are defined for the gaming platform, the player database and the payments system, and the date and result of each continuity test are recorded by the Information Security lead.

15.2 Wind-down

The CGA publishes wind-down templates for B2C and B2B licensees. The Company maintains a wind-down plan providing for orderly cessation: notification to the CGA and to players; suspension of new registrations and deposits; settlement or voiding of open wagers; return of all player balances from the segregated account; retention and secure handover of records; and termination of supplier relationships.

15.3 Records and retention

Record class	Minimum retention
CDD/EDD documents, account files, business correspondence	5 years after the end of the business relationship
Transaction records (domestic and international)	5 years, sufficient to permit reconstruction of individual transactions
Internal and external unusual transaction reports	5 years
Age verification processes and outcomes	Retained and available for regulatory review
Operator-initiated exclusion records	At least 5 years
Self-exclusion records	Per applicable retention periods; payment methods blocked during the exclusion period where possible
Complaint and dispute records	5 years, or the shorter period stipulated by data protection, limitation or other applicable law
Responsible gaming interactions and interventions	Recorded in the PAM system; retained per the above
Training records	At least 5 years
Gaming and transaction logs	Per the LOK, license conditions and CGA instructions; documented log-retention periods
Communications relating to participation in games	5 years — to be stated in the General Terms & Conditions under Article 11(3)(g)

Data protection law does not override these obligations for the record classes above. Secure disposal at end of retention uses appropriate deletion, cryptographic erasure, overwriting or physical destruction.

16. Compliance Monitoring and Assurance

16.1 Three lines

Line	Function	Activity
First	Operations — customer support, KYC, payments, VIP, marketing, technology	Executes the controls; performs day-to-day checks; escalates flags and internal reports
Second	Compliance — NOGC Compliance Officer, AML/CFT Compliance Officer, Responsible Gaming Officer, Information Security lead	Sets policy, monitors adherence, performs thematic reviews, owns regulatory reporting
Third	Independent audit and CGA-approved independent experts	Tests the design and operating effectiveness of the control framework; independent of first and second lines

16.2 Compliance calendar

Frequency	Activity
Daily	Segregated player-funds reconciliation; transaction monitoring alert triage; responsible gaming flag review
Weekly	Unauthorised device detection process; open incident and remediation review
Monthly	Software support status check; vulnerability scanning; patching; liquidity confirmation; player-fund reconciliation sign-off
Quarterly	User, administrator and service account review; Board review of compliance findings, incidents and overdue remediation; permitted-market list review
Twice yearly	Formal asset and software inventory review; complaints reports to the CGA on 15 January and 15 June
Annually	Business Risk Assessment and Customer Risk Assessment refresh; information security risk assessment; CIS IG1 self-assessment; business continuity and disaster recovery test; verification of game, RNG and platform certifications; Responsible Gaming effectiveness report; all-staff training; review and re-approval of this Manual
On event	Incident report within 24 hours; change report; critical change permission before implementation; unusual transaction report to the FIU without delay

16.3 Obligations register

The Company maintains an applicable-obligations register covering gaming, information security, privacy, AML/CFT/CPF and relevant contractual requirements, mapping each obligation to its source, its owner, the control that satisfies it and the evidence retained. Annex C of this Manual is the summary view of that register.

16.4 Non-compliance

Suspected breaches of this Manual must be reported promptly to Senior Management and to the NOGC Compliance Officer. The Company may take proportionate corrective or disciplinary action, up to and including termination of employment or contract. Failure to comply with the LOK or with any provision of the license may result in administrative measures imposed by the CGA, including administrative fines, compliance directives, suspension and revocation of the license.

16.5 Review and approval

This Manual is issued in July 2026 as a draft for review by the Board of Directors. It has not been approved and is not in force; no effective date applies at this stage. On approval the Board will record the date of approval and set the effective date, and this section, the Document Control table and the version history will be updated accordingly. Once in force the Manual is reviewed at least annually from its effective date, and earlier following a material legal, regulatory, organisational, system, supplier or threat change, or a material incident. Amendments require approval by the Board of Directors. Each version is recorded in the version history below.

Version	Date	Author	Approved by	Summary of change
1.0 — Draft	July 2026	NOGC Compliance Officer	Not yet approved — pending Board of Directors	Initial draft issued for Board review. Not in force; no effective date.

Annex A — Roles and Responsibilities Summary

Area	Accountable	Responsible	Consulted / Informed
This Manual	Board	NOGC Compliance Officer (Ivaylo Stamchev)	All key persons
KYC / CDD / EDD	AML Compliance Officer	KYC team	NOGC Compliance Officer, Customer Support
Player funds and payments	Managing Director	Board member responsible for Payments	Board, Compliance Officer
Responsible gaming	Board	Board member responsible for Responsible Gaming	Customer support and VIP frontline staff
AML/CFT/CPF	Board	Compliance Officer (Ivaylo Stamchev)	FIU, independent auditor
Information security	Board	Board member responsible for Information Security	AWS and platform providers
Account suspension and closure	NOGC Compliance Officer	Relevant function per Section 9.1	Customer Support
Game and RNG certification	NOGC Compliance Officer	Technology / Product	Testing laboratories, CGA portal
Supplier approval and oversight	Managing Director	NOGC Compliance Officer	CGA, Legal
Complaints and ADR	NOGC Compliance Officer	Board member responsible for Customer Support	EGIS – FZCO (ADR), CGA
Regulatory reporting	NOGC Compliance Officer	Function owner per Section 14.1	Board, CGA
Business continuity and wind-down	Board	Managing Director	All functions, CGA

Annex B — Key Thresholds and Deadlines

Item	Value	Source
CDD verification threshold	NAf. 4,000 cumulative deposits and withdrawals, calculated daily	CGA AML/CFT Regulations III.3
Deadline to obtain information after threshold reached	30 days, else terminate the relationship	CGA AML/CFT Regulations III.3
Additional payout verification	Payouts cumulatively exceeding EUR 2,300	Account, Pay-outs and Bonuses policy
Minimum legal gambling age	18	LOK Article 1.4(d)
Incident report to CGA	Within 24 hours	License conditions Article 13(3)
FIU response to information request	Promptly — within 5 working days	AML Policy
Complaint window	6 months from bet settlement or incident	CGA Complaints Policy 3.1
RG complaint acknowledgement	2 days	CGA Complaints Policy 4.1
RG complaint resolution	5 business days, extendable by 2 weeks	CGA Complaints Policy 4.1
Other complaint acknowledgement	7 days	CGA Complaints Policy 4.2
Other complaint resolution	4 weeks, extendable once by 4 weeks	CGA Complaints Policy 4.2
Complaints reports to CGA	15 January and 15 June	CGA Complaints Policy 6
Cooling-off durations	24 hours, 7 days, 1 month, 3 months	CGA RG Policy 9.1.2
Self-exclusion durations	1, 3, 5, 10 years, lifetime — minimum 1 year	CGA RG Policy 9.2.2; LOK 5.4(2)
Deposit limit — more severe	Immediate effect	CGA RG Policy 10.1
Deposit limit — less severe	24-hour waiting period	CGA RG Policy 10.1
Exceptional RG request via email/chat	Enabled within 24 hours	CGA RG Policy 9.1 / 9.2
Player transaction history in account	At least 90 days	License conditions Article 9(9)(e)
Player self-assessment history	At least 6 months; longer on request within 10 working days	CGA RG Policy 7
Winnings availability	Not less than 30 months from award	License conditions Article 9(9)(g)
Record retention (AML, transactions, CDD)	At least 5 years	CGA AML/CFT Regulations IV.3
Operator-initiated exclusion records	At least 5 years	CGA RG Policy 9.3
RG effectiveness report to management	At least every 12 months	CGA RG Policy 3
Compliance Officer CPD	At least 10 hours per year	CGA Compliance Officer Requirements 4
Compliance Officer operator cap (outsourced)	No more than 10 operators	CGA Compliance Officer Requirements 8

Annex C — Requirement to Manual Mapping

Article references are to the CGA license conditions for an indefinite-term online gaming license, effective 17 December 2025, as applied to license OGL/2024/659/0586 held by Trigonon Group N.V. for www.goal365.bet.

Requirement	Source	Addressed in
Customer identification and verification	Art. 14(1)(a)	Section 4
Player account and fund management	Art. 14(1)(b)	Section 5
Responsible gaming	Art. 14(1)(c)	Section 6
Information security	Art. 14(1)(d)	Section 8 + Information Security Policy
AML/CFT/CPF	Art. 14(1)(e)	Section 7
Suspension and closure of player accounts	Art. 14(1)(f)	Section 9
Safe and secure environment; impeccable conduct; liquidity and ring-fencing	Art. 6	Sections 3.1, 5.4, 8
Equipment and application software; inventory	Art. 7	Section 10
Player registration; intermediaries	Art. 8	Sections 4.1, 5.3
Payment transactions; segregation; currency; account information	Art. 9	Sections 5.2–5.5
Game certification by CGA-approved test lab; supplier disclosure	Art. 10	Section 10.1
General terms and conditions — mandatory content	Art. 11	Section 12.1
Publicly accessible information; CGA digital seal	Art. 12	Section 12.2
Reporting and data access; 24-hour incident clock; Tier-IV data centre	Art. 13	Sections 8.6, 14
Critical change consent	Art. 4	Section 14.3
Prior CGA approval of platform, game and payment suppliers	Art. 2(6)	Section 11.1
Outsourcing does not remove accountability	Art. 3(2)	Sections 1.2, 11
Consequences of violations	Art. 15	Section 16.4

Annex D — Reference Documents

Legislation and license

- National Ordinance on Games of Chance (Landsverordening op de kansspelen, PB 2024 no. 157, "LOK"/"NOGC"), as amended.
- CGA license conditions for an indefinite-term online gaming license, effective 17 December 2025.
- Ordinance on the Notification of Unusual Transactions (NORUT).
- National Ordinance on Identification in Service Provision (NOIS).
- Sanctions National Ordinance (SNO).
- National Ordinance on the Protection of Personal Data.

CGA policies and guidelines

- Responsible Gaming Policy for Licensed Operators, v1.0, 17 April 2025.
- Player Complaints Policy Guidelines, v1.1, 18 June 2025.
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, January 2025.
- GCB/CGA Requirements for Compliance Officer based on NOIS/NORUT.
- Information Security Control Requirements for CGA Licensees (CIS Controls Implementation Group 1).
- Alternative Dispute Resolution policy and ADR Role and Certification Guidelines.
- Crypto Policy.
- Wind Down template (B2C).

Company policies published at www.goal365.bet

- General Terms & Conditions.
- Responsible Gaming.
- Self Exclusion.
- Gaming Addiction.
- Player Complaints and Dispute Resolution Policy.
- Anti-Money Laundering Policy.
- KYC Policies, Privacy & Management of Personal Data.
- Account, Pay-outs and Bonuses.
- Fairness & RNG Testing Methods.
- Refund Policy.
- Cookies Policy.
- Betting Rules / Netting Rules.

Company internal documents

- CGA Certificate of Operation for www.goal365.bet — license OGL/2024/659/0586, granted 23 May 2025.
- Information Security Policy, v1.0 (July 2026).
- Business Risk Assessment and Customer Risk Assessment.
- Transaction monitoring rule set and escalation matrix.
- Supplier register, certification register and equipment inventory.
- Wind-down plan on the CGA B2C template.

— END OF MANUAL —