FOR YOUR COMPLIANCE TEAM

Security and data pack

One page for a broker's compliance or IT due diligence, including DORA ICT third-party checks for EU-licensed brokers. Fields in [brackets] are filled in before sending. Everything below is a **commitment of how the service runs**, not a certification: the operator holds no ISO 27001 or SOC 2 certificate today.

Provider: [legal entity], operated by Alvaro [surname] · **Service:** Risk & Abuse Radar (Leak Audit; Radar + Action Desk) · **Contact:** [email] · **Incident line:** [phone / Signal]

1. What data we receive

RECEIVED	NEVER RECEIVED
Account login, MT5 group, leverage, swap-free flag, IB id	Names, emails, phone numbers, addresses
Deals: time, symbol, side, volume, price, profit, swap, commission, position id	IP addresses, devices, geolocation
Balance operations: type, amount, time	KYC documents, payment methods, card or bank data
Symbol settings and the economic calendar	Passwords of client accounts

If an export or feed contains personal fields, they are **dropped on arrival** and never stored. Logins are pseudonymised in everything shared beyond the broker's own reports. That includes alerts posted to shared channels and any data sent to an AI model.

2. How we access it (access ladder)

1. **Leak Audit:** a one-off CSV export, sent encrypted, after an NDA.
2. **Live Radar:** a **read-only manager login** created by the broker on its own server. It is restricted to client groups and to the Radar's static IP [x.x.x.x]. We never request administrator rights.
3. **Optional, later:**
   - a **broker-side executor**, where the broker applies dealer-approved actions with its own credentials, or

- a **scoped write manager** with account edits only (leverage, group, trading rights), IP-locked, every action logged, after a shadow period.

Neither includes balance operations or closing positions.

The broker can revoke access at any time by disabling the manager login. The service then stops at once.

---

3. Where and how it is stored

- **Hosting:** cloud provider, region EU region. A dedicated instance, with disks encrypted at rest.
- **In transit:** TLS for all connections. Exports arrive in AES-256 encrypted archives.
- **Separation:** each broker's data is held in its own storage location and is never mixed with another broker's or used to benchmark them by name.
- **Access:** only the operator, with MFA on every account. No shared credentials.
- **Logs:** access to data and every recommended and executed action are logged with time and approver, and kept for 24 months.

---

4. Retention and deletion

- **Leak Audit exports:** deleted within **30 days** if the broker does not sign. A deletion confirmation is sent on request.
- **Live service:** raw data is kept for a rolling 12 months. Reports and evidence packs are kept for the contract term plus 12 months for dispute support.
- **On termination:** all data is deleted within **30 days**, with written confirmation. An export of the broker's reports is provided on request first.

---

5. Sub-processors

SUB-PROCESSOR	PURPOSE	DATA IT SEES	LOCATION
cloud provider	Hosting and storage	All received data, encrypted	EU
LLM provider	Drafting evidence stories, briefs and dossiers	Pseudonymised case data only; no logins in clear, no personal data	region; no training on customer data under the provider's API terms
Telegram / Slack	Alert delivery to the dealer	Pseudonymised alert text	Provider's

Abuse detection itself is **rule-based and runs on the operator's own instance**. No AI model decides whether an account is flagged.

---

6. Incidents

- **Notification:** suspected or confirmed incidents affecting the broker's data are notified within **24 hours**. The notice covers what happened, the data affected, the containment taken and the next steps.
- **Contact:** name, email, phone, monitored hours.
- The broker's own incident contact is recorded at onboarding.

---

7. DORA register information (EU brokers)

For the broker's register of ICT third-party arrangements:

ITEM	VALUE
Function supported	Trading-risk analytics; abuse-indicator alerts (does not support execution or client money)
Critical or important function?	Broker's assessment; typically **no**, as the service is advisory and read-only by default
Data location	EU region
Sub-contracting	Section 5
Exit strategy	Revoke the manager login; data deleted within 30 days; reports exportable
Audit and access rights	The broker may request evidence of the controls above, and a remote walkthrough, once a year or after an incident

---

8. Business continuity

- One operator. If the operator is unavailable, alerts stop. The broker's own risk tools and dealers stay in place, so there is no dependency on the Radar for trading.
- Configuration and Rulebook are backed up daily provider, region. The service can be restored on a new instance within 2 working days.

Prepared date*. Reviewed yearly or when a sub-processor changes.*