Incident and Data Breach Management Procedure

KYCJet — GREM S.R.L. Supporting the customer's obligations under Article 33 GDPR (notification to the supervisory authority within 72 hours) and Article 19 of Regulation (EU) 2022/2554 with Commission Delegated Regulation (EU) 2025/301 (initial notification of a major incident within 4 hours of classification and in any event within 24 hours of becoming aware of it). Version of 21 September 2026.

1. Why our deadlines are shorter than yours

The customer must notify its authorities within hours, and can only do so with the information we give it. That is why our deadlines towards the customer start from when we detect the incident, not from when we have understood everything.

2. What an incident is

- **ICT incident**: an event that compromises the availability, authenticity, integrity or confidentiality of the Service or of the data it processes (for example unavailability, errors in verifications, unauthorised access, a provider that does not respond).
- **Personal data breach**: an incident that leads, even potentially, to the accidental or unlawful destruction, loss, alteration, disclosure of, or access to, the data of verified persons (Article 4(12) GDPR).

3. How we detect incidents

- Automatic alerts on critical failures, sent to the on-call channel.
- External availability monitoring [to be activated].
- Log of staff access to cases and log of interface calls.
- Reports from customers, verified persons or providers, to **security@gremcompany.com**. The address is also published at `/.well-known/security.txt` (RFC 9116), which is where whoever finds a flaw looks first. Whoever reports in good faith and does not make the damage worse is not pursued.

4. Roles

Role	Who	Tasks
Incident lead	[Name, role] — deputy: [Name]	Classifies, decides, communicates with customers
On-call engineer	[Rota]	Contains, investigates, restores
Privacy lead	[Name]	Assesses whether there is a data breach and its risks

5. Phases and deadlines towards the customer

Phase	Deadline, from when we detect it	What we do
Detection and containment	Immediately	We stop the damage: credential revocation, blocking functions, isolation
First communication	Within **[2 hours]** if the incident affects the Service or the data	What happened as far as we know, which customers and data are affected, what we have already done, who the contact person is
Data breach notification	Without undue delay and in any event within **[24 hours]**	The information under Article 33(3) GDPR available: nature of the breach, categories and approximate number of data subjects and records, likely consequences, measures taken or proposed
Intermediate update	Within **[48 hours]**, then whenever something material changes	Causes, updated impact, recovery status. Supports the DORA intermediate report (within 72 hours of the initial notification)
Final report	Within **[20 days]** of resolution	Root cause, overall impact, permanent measures. Supports the DORA final report (within one month)

Communications go to the security contact the customer sets in its organization settings (email and certified email), and for critical incidents also by phone. If no contact is set we write to whoever opened the organization: setting it is the customer's job, and the dashboard says so.

6. What we do not do

- We do not notify the supervisory authority or the customer's authorities on its behalf, and we do not contact verified persons, unless the customer instructs us in writing: the customer is the controller and the supervised entity.
- We do not wait until we have all the information before the first communication.

7. After the incident

Every incident, even without consequences, is recorded with date, duration, causes, impact and measures. Lessons learned become changes to the Service or to this procedure. The register is available to customers and their authorities, for the part that concerns them.

8. Testing

The procedure is tested [once a year] with an exercise on a realistic scenario, and after every major incident.