TEMPLATE P51 · INCIDENT REPORTS AND COMMUNICATIONS

Incident reports and communications

Documents the decision whether to report under each regime applicable to an AI incident, prepares the common content of reports and the communications to affected persons, employees and customers, and tracks their time limits.

Fernando García Varela Version 0.1 (working draft) 19-09-2026 Draft for review

IN THIS DOCUMENT

01 Instructions for use

02 Identification

03 Decision whether to report

04 Common content of reports

05 Serious incident report (AI Act)

06 Personal data breach notification (GDPR)

07 DORA and NIS2 reports

08 Communication to affected persons

09 Internal and customer communication

10 Register of reports and communications

11 Quality criteria

12 Approval and verification

13 Version control

Legal notice and disclaimer. SEVEN-G is a reference methodological framework provided "as is" and for information purposes only. It does not constitute legal, regulatory, financial or professional advice, nor does it guarantee compliance with any law or standard. References to general regulation (such as the EU AI Act, the GDPR, DORA or NIS2), to technical standards and to regulation specific to each sector or jurisdiction may be incomplete, may not apply to a particular case or may become out of date as a result of regulatory changes, interpretations or supervisory positions after their consultation date. **Each organisation that uses SEVEN-G is solely responsible for identifying the regulation that applies to it, verifying that it is current and certifying its own regulatory compliance**, with the appropriate qualified advice. This methodology is a generic, free aid shared with the community so that nobody has to start from scratch; each person or organisation can and should adapt it to its own use. It must not be inferred that its legally sensitive parts have been reviewed by legal counsel: those reviews, for each company or sector, are the ultimate responsibility of the company, consultant or organisation that uses it. Although every effort is made to keep it up to date, some regulation may have changed without being reflected here. To the fullest extent permitted by law, the author accepts no responsibility whatsoever for the effects of its application in any organisation or for its full applicability. The methodology does not grant certification of any kind. The author accepts no liability for any use made of this content or for any decisions taken on the basis of it. The data, figures, companies and cases in the examples are fictitious or illustrative.

Why it matters. A single AI incident can trigger the AI Act, the GDPR, DORA and NIS2 at the same time, each with its own clock, which starts upon awareness and not when the analysis is finished. Omitting or delaying a mandatory report is a critical nonconformity (01 §12), and not reporting without recording why is indefensible before a supervisor. This template requires all regimes to be assessed in parallel, the decision not to report to be reasoned in writing, and the messages to affected persons, employees and customers to be ready before they are needed.

01

Instructions for use

Aspect	Guidance
When it is used	The models in sections 5 to 9 are adapted to the system in phase 5, together with the incident response plan (P26), before G5. For each incident, section 3 is opened at triage and the register in section 10 is kept until the final report under each regime.
Who completes it	The AI Risk Owner and compliance assess the regimes; the data protection officer, personal data breaches; the incident coordinator provides the facts; corporate communications drafts the messages.
Who verifies it	Legal counsel validates every report, every external communication and every reasoned decision not to report. Under Enterprise, the AI Auditor reviews the register at R6.
Who decides or approves	The report is submitted by whoever the rule designates (provider, controller, financial entity, essential or important entity). Internally, it is signed by the person designated in plan P26; for S1, with the knowledge of the AI Sponsor and the board committee (37 §4.3).
Stage, *gate* or moment	Preparation before G5 (G5.17). Use in phase 6 during each incident. Review at R6 (R6.06), in the annual S1 drill (37 §5) and in C4.
Tool	T08 · Nonconformity and incident register: reporting clocks and alerts. This template holds the content that T08 does not draft.
Reference document	Document 37 §4.5 (phases 5 and 6) and §5 (regimes, time limits and rules); document 34 (regime applicable to each system); document 36 (reporting by suppliers).
Lite versus Enterprise	The assessment of all regimes and the reasoned decision not to report are mandatory in both. Lite may omit the fields marked **(Enterprise)**.

Completion rules:

- **Official forms prevail.** Where an authority publishes its own form, template or channel, that one is used and this template only serves to prepare the content. For Art. 73 of the AI Act there is the Commission's Draft guidance and template on serious incident reporting (34 §3.3); DORA has forms in its implementing measures, and supervisory authorities and CSIRTs have their own channels. This template neither reproduces nor replaces any of them.
- Time limits are taken from document 37 §5 and confirmed with legal counsel at the time of the incident; this template does not set time limits of its own.
- The clock for each regime starts at the date and time of detection recorded in T08 or at the moment the rule specifies; never at the end of the analysis.
- Where the rule provides for it, an incomplete initial report submitted on time is preferable to a complete report submitted late.

- Every external communication distinguishes confirmed facts from ongoing assessments and does not speculate about causes.
- An AI incident that is also a breach or a security incident is managed **only once**, with a single coordinator (37 §1).

This template does not constitute legal advice (reference consultation date of the framework: September 2026).

02

Identification

Field	Content	Guidance
Incident		INC-AAAA-NNN (P27, T08).
System and use case		SIA-AAAA-NNN · IA-AAAA-NNN.
Current severity		S1 · S2 · S3 · S4 (37 §4.2).
Date and time of detection		Start of the clocks.
Company's role in relation to the system		Provider · Deployer · Both (P11, document 34).
Role in relation to personal data		Controller · Processor · Not applicable.
Subject to DORA · to NIS2		Yes · No · To be determined (P26 §2).
Incident coordinator		
Person responsible for the regulatory assessment		AI Risk Owner and compliance.

03

Decision whether to report

One row per regime. It is assessed **in parallel with containment**. Where the answer is No, the reasoning is mandatory.

Regime	Applies? (Yes · No · To be determined)	Criterion assessed	Decision (Report · Do not report · Pending)	Reasoning	Decided by	Validated by Legal	Date and time
AI Act, Art. 73 (serious incident in a high-risk system)		Serious incident under Art. 3(49)? High-risk system? Company's role?					
AI Act, Art. 26(5) (deployer informing the provider)		Does the company deploy a third party's high-risk system?					
GDPR, Art. 33 (supervisory authority)		Personal data breach? Is it unlikely to result in a risk to rights and freedoms?					
GDPR, Art. 34 (data subjects)		Is a high risk to individuals likely?					
DORA, Art. 19		Major ICT-related incident under its classification criteria?					
NIS2, Art. 23		Significant incident under the national transposition?					
Sector-specific regulation		Sector supervisor or public sector security scheme (P02).					

Regime	Applies? (Yes · No · To be determined)	Criterion assessed	Decision (Report · Do not report · Pending)	Reasoning	Decided by	Validated by Legal	Date and time
Contractual obligations		Contracts with customers or suppliers.					
(illustrative example) **GDPR, Art. 33**	Yes	Contact details of 40 customers visible to another customer for 20 minutes	Report	Risk not unlikely: identifying data exposed to an unauthorised third party	Data protection officer	Yes	12-11-2026 18:30

3.1 Reasoned decision not to report

One for each regime assessed as Do not report. It is kept even if the incident is closed without consequences.

Field	Content	Guidance
Regime		
Facts considered		What was known at the time of the decision, with date and time.
Regulatory criterion applied		Why the threshold is not met (for example, it is not a high-risk system; the breach is unlikely to result in a risk; the classification criteria are not reached).
Uncertainties		What is not yet known and what would change the decision.
Planned review		When the decision is reviewed if new facts emerge.
Decided by · validated by		Role, name, date; validation by legal counsel and, for breaches, by the data protection officer.

04

Common content of reports

Basis for completing any official form. Each regime asks for a subset and uses its own format.

Field	Content	Guidance
Reporting entity and contact		Company name, contact person, data protection officer where applicable.
Internal reference		INC-AAAA-NNN.
Dates and times		Estimated start, detection, classification, containment.
System affected		Name, version, supplier, purpose, company's role.
Description of the incident		What happened, in plain language.
People and data affected		Number and categories, approximate if not known exactly. *No data* if unknown.
Likely consequences		By impact axis (33 §4.2).
Causal link with the system		Established · Reasonable likelihood · Under analysis (relevant to Art. 73).
Measures taken and planned		Containment, mitigation for the people affected, correction.
Cross-border effect		Member States affected.
Evidence preserved		Logs, versions and configurations preserved before the system is modified (37 §4.5; Art. 73(6) for high-risk providers).
Nature of the report		Initial · Intermediate · Final · Supplement to an incomplete report.

05

Serious incident report (AI Act)

Field	Content	Guidance
Who reports?		Provider of the high-risk system. If the company is a deployer, it **immediately** informs first the provider and then the importer or distributor and the market surveillance authorities (Art. 26(5)).
Recipient		Market surveillance authority of the Member State where the incident occurred; the EU AI Office for systems within its competence (37 §5).

Field	Content	Guidance
Time limit case		General: not later than 15 days · Widespread infringement or serious and irreversible disruption of critical infrastructure: 2 days · Death: 10 days. From becoming aware.
Date and time of becoming aware		
Calculated deadline		Confirmed by legal counsel.
Incomplete initial report		Yes · No. What is missing and when it will be completed.
Limited regime due to equivalent sector-specific reporting		Yes · No, with justification (Art. 73(9) and 73(10)).
Form used		Official template in force or the authority's channel; version and date.
Temporal applicability		The obligations for the high-risk systems listed in Annex III apply from 2 December 2027; until then, the serious incident criterion is the internal S1 threshold and the assessment is documented (37 §5).

06

Personal data breach notification (GDPR)

Field	Content	Guidance
Competent supervisory authority		In Spain, the Spanish Data Protection Agency , except for cross-border processing with another lead authority.
Date and time of becoming aware		
72-hour deadline		If notified later, reasons for the delay.
Content		Nature of the breach; categories and approximate number of data subjects and records; contact details of the data protection officer; likely consequences; measures taken or proposed, including mitigation measures. If not all the information is available, it is provided in phases.
Processor involved		Date on which it notified the company.

Field	Content	Guidance
Internal documentation of the breach		All breaches are documented, whether or not they are notified.

07

DORA and NIS2 reports

By reference only: the official forms and channels are used. This table follows the phases and time limits of 37 §5.

Regime	Phase	Reference time limit (37 §5)	Deadline	Sent (date and time)	Authority reference
DORA	Initial notification	4 hours from classification as major and not later than 24 hours after becoming aware			
DORA	Intermediate report	72 hours from the initial notification			
DORA	Final report	One month after the latest intermediate report			
DORA	Information to clients	When the incident affects their financial interests			
NIS2	Early warning	24 hours			
NIS2	Incident notification	72 hours			
NIS2	Final report	One month after the notification			

For financial entities, DORA acts as sector-specific legislation with respect to NIS2 for incident reporting; the regime is confirmed in document 34.

08

Communication to affected persons

Mandatory where the GDPR requires it (likely high risk to individuals) and advisable where the incident affects their decisions or interests even if no rule requires it **(Enterprise)**.

Element of the message	Content	Guidance
What happened		Clear and plain language, without jargon.
Which data or decisions affect them		
Possible consequences		Without minimising or causing alarm.
What the company has done		Containment and correction.
What they can do		Recommended protective measures; human review of affected decisions.
Contact		Data protection officer or a specific point of contact.
Channel and date sent		

(illustrative example) "On 12 November, for about 20 minutes, an error in our enquiries assistant displayed your name and telephone number to another customer. We have corrected the fault and the assistant now operates with additional controls. No bank details or passwords were visible. If you receive unexpected calls on behalf of the company, do not provide any data and contact our data protection officer through the usual channel."

09

Internal and customer communication

Recipient	Timing	Minimum content	Author	Validated by	Sent
AI Committee	S1: 4 hours · S2: 24 hours (37 §4.3)	What happened, who is affected, what has been contained, reports made or within time limits, decisions that may be required	Coordinator	AI Risk Owner	

Recipient	Timing	Minimum content	Author	Validated by	Sent
Board committee	S1: 24 hours	As above, with confirmed facts separated from assessments (37 §9)	AI Sponsor	AI Committee	
Employees who use or oversee the system	Upon containment	What changes in their work, fallback process, whom to consult	AI Product Owner	Communications	
Affected customers (other than natural persons) (Enterprise)	As per contract or where appropriate	Facts, effect on the service, measures, contact	Communications	Legal	
Suppliers involved	At triage	Facts, request for information and for preservation of evidence (36 §6)	AI Technical Owner	Legal	
Public communication (Enterprise)	Only where appropriate	Single coordinated message	Communications	Legal and AI Sponsor	

10

Register of reports and communications

One row per submission. Rows are identified by the incident code and a sequence number (INC-AAAA-NNN · N*nn*).

No.	Regime or recipient	Type (initial · intermediate · final · communication)	Clock from (date and time)	Deadline	Sent (date and time)	On time?	Acknowledgement reference	Owner
N01								
N02								
(illustrative example) **INC-2026-021 · N01**	GDPR · supervisory authority	Initial	12-11-2026 17:10	15-11-2026 17:10	13-11-2026 11:40	Yes	Electronic office acknowledgement	Data protection officer

A late or omitted report opens a critical nonconformity in P50, in addition to any revealed by the incident (37 §6).

11

Quality criteria

Formal criteria in document 21 (G5.17 and R6.06) and process in document 37.

#	Check	Status
1	All regimes have been assessed in parallel with containment, with date and time.	Met · Not met · Not applicable · Pending
2	Each decision not to report is reasoned, dated and validated by legal counsel.	
3	Time limits are calculated from the moment of awareness and confirmed by legal counsel.	
4	The official forms or channels in force have been used where they exist.	
5	Communications distinguish confirmed facts from ongoing assessments and have been validated.	
6	The register makes it possible to demonstrate for each submission that it was made on time.	
7	Missed time limits have an open nonconformity in P50.	

12

Approval and verification

Function	Role in SEVEN-G	Name and position	Date	Signature or reference
Assesses the regimes	AI Risk Owner and compliance			
Assesses breaches and communicates with data subjects	Data protection officer			
Provides the facts	Incident coordinator			

Function	Role in SEVEN-G	Name and position	Date	Signature or reference
Drafts the communications	Corporate communications			
Validates	Legal counsel			
Reviews the register at R6	AI Office (Lite) · AI Auditor (Enterprise)			

Segregation of duties: whoever decides not to report does not validate their own decision; validation is carried out by legal counsel.

13

Version control

Completed document

Version	Date	Author	Changes

Template

Version	Date	Changes
0.1	19-09-2026	First version. Decision whether to report with a reasoned decision not to report, common content, AI Act and GDPR reports, reference to DORA and NIS2, communications to affected persons, internal and customer communications, and a register of time limits in accordance with 37 §5.

External sources cited

Links to the official or primary source, checked before publication. Always verify the version in force on the date of use.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) · https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng · Parlamento Europeo y Consejo de la UE · 14-12-2022

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng · Parlamento Europeo y Consejo de la UE · 27-04-2016

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA) · https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng · Parlamento Europeo y Consejo de la UE · 14-12-2022

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) · https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng · Parlamento Europeo y Consejo de la UE · 13-06-2024

European AI Office (European Commission) · https://digital-strategy.ec.europa.eu/en/policies/ai-office · Comisión Europea (DG CONNECT)

Spanish Data Protection Agency (Agencia Española de Protección de Datos, AEPD) · https://www.aepd.es/en · Agencia Española de Protección de Datos

Draft guidance and reporting template on serious AI incidents (Article 73 AI Act) · https://digital-strategy.ec.europa.eu/en/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks · Comisión Europea · 26-09-2025