

ZInfV-1

Readiness checklist

A practical overview of key duties for essential and important entities.

ORGANISATION	REVIEW DATE	RESPONSIBLE PERSON

How to use: tick implemented measures; add outstanding items to an action plan.

01 Identifying your obligations

Arts. 6, 7 and 8

- ☐ We reviewed our sector, activities, size and the specific ZInfV-1 criteria.
- ☐ We determined essential or important entity status and documented why.
- ☐ If in scope, we completed self-registration or checked the deadline.

02 Management accountability

Arts. 20 and 22

- ☐ Management approved security measures and oversees their implementation.
- ☐ Information security is included in our annual business or work plan.
- ☐ Management trains at least every 4 years; ICT administrators annually.
- ☐ Employees receive regular information security training.

03 Security documentation

Art. 21

- ☐ We have a security policy and an up-to-date asset inventory.
- ☐ Our risk analysis documents the methodology and acceptable risk level.
- ☐ We have a business continuity plan and a business impact analysis.
- ☐ System recovery and incident response plans are in place.
- ☐ Security measures and their effectiveness reviews are documented.

What does a ticked item mean?

A measure is documented, implemented, maintained and evidenced in practice.

Implementation and follow-up

The remaining checklist items and the next practical steps.

04 Security measures in practice

Art. 22

- ☐ We manage identities, user access rights and privileged accounts.
- ☐ We back up data and test our ability to restore it.
- ☐ We manage vulnerabilities, application security and malware protection.
- ☐ Key suppliers have defined and verifiable security requirements.
- ☐ Physical security, secure communications, encryption and MFA are risk-based.

05 Event logging

Art. 24

- ☐ We log key access, changes, security events and administrator activity.
- ☐ Logs are protected, time-synchronised and kept for at least 6 months.

06 Incident response and reporting

Arts. 29 and 30

- ☐ We defined significant-incident criteria and internal escalation steps.
- ☐ We know our CSIRT and the 24-hour warning / 72-hour reporting rules.
- ☐ Procedures cover interim, final and follow-up incident reports.

07 Compliance assessment

Art. 25

- ☐ Essential: compliance audit; important: self-assessment at least every 2 years and after a significant incident.
- ☐ Nonconformities have owners, deadlines and evidence of remediation.

GENERAL DEADLINE (ARTS. 21 AND 22)

19 DEC 2026

SIGNIFICANT INCIDENT

24 h / 72 h

Exceptions: certain previously designated entities, state bodies and telecom operators had a 19 June 2026 deadline; special sector rules may apply.

NEXT ACTION

OWNER / DUE DATE

[ZInfV-1 \(official text\)](#)

| [URSIV: official guidance](#)

Informational aid only; not a substitute for the law or legal advice. Unofficial English text.