GDPR

GDPR (whole Part)

Audit Checklist

381 audit questions across **46** sections.

HOW TO USE THIS CHECKLIST

Each question has three boxes the auditor fills in during the audit:

1. **Compliance** — the binary headline: Compliant / Non-compliant.
2. **Classification** — where the gap is, four-state grid: Documented / Implemented matrix.
3. **Finding level** — severity: Maj / Min / Obs (Major nonconformity / Minor nonconformity / Observation).

Severity is the auditor's call on the day, against the real finding — no severity is pre-suggested per question.

auditchecklists.org Audit Checklist Licence

Product:	GDPR (whole Part) (381 questions)
Regulation:	
Issued:	[YYYY-MM-DD — STAMPED AT ISSUE]

Licensed to:	[ORG NAME — STAMPED AT ISSUE]
Licensee email:	[EMAIL — STAMPED AT ISSUE]
Order:	[AVI-YYYY-NNNNN — STAMPED AT ISSUE]

Licence terms

This audit checklist is licensed for use within the organisation named above by the licensee email named above. Use is permitted by employees and contractors of the named organisation in the course of their work for that organisation, including printing, internal distribution within the organisation, annotation during audits, and incorporation into the organisation's management-system documentation as a working reference.

Not for redistribution. Sharing this document, or any derivative or extract of it, with any party outside the named organisation is a breach of this licence. This includes posting to file-sharing networks, internal wikis or knowledge bases accessible to other organisations, vendor portals, supplier-facing GRC systems, and email forwarding to colleagues at other firms. Quoting individual audit questions in regulator submissions or internal training materials is permitted; reproducing the structured checklist as a whole is not.

Each additional organisation or operating site requires a separate licence. If a sister organisation in the same group, or a separate operating entity, requires the same checklist, contact licences@auditchecklists.org for a multi-site licence quote. Holding companies licensing for multiple subsidiaries are eligible for group-licence pricing.

Licence transfers. This licence does not transfer with sale, merger, or organisational restructure without written consent. auditchecklists.org may, at its discretion, transfer the licence to the successor organisation on request — usually a formality, contact licences@auditchecklists.org.

Defects and amendments. If you identify a defect in this checklist — wrong content, mistranscribed regulation, factual error — email support@auditchecklists.org. We will verify the defect, correct it, and reissue the affected artefacts to you within a reasonable timeframe at no further charge. Regulatory amendments published during your 12-month update

§Article 2

Material scope

Q1 ARTICLE GDPR Art.2(1)

Has the organisation identified every processing activity it carries out and confirmed that each is either (a) wholly or partly automated, or (b) non-automated but forming or intended to form part of a structured filing system?

SOURCE VERBATIM

> 1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
>
> — Regulation (EU) 2016/679 Article 2(1), Consolidated 2016-05-04 (GDPR)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- The processing inventory (ROPA, Art. 30) — every processing activity classified as automated, non-automated-filing-system, or out-of-scope
- Description of any non-automated records: how they are organised, indexed, and retrieved
- For activities classified as out-of-scope: the rationale
- Sample of physical record-keeping (HR personnel files, contract files, customer files) — confirmation that the structured nature was assessed
- Process for new processing activities: scope determination as a step before processing begins

MANAGEMENT SYSTEM REFERENCE: _____

FINDINGS / NOTES:

Q2 ARTICLE GDPR Art.2(2)(a)

For any processing the organisation has classified as outside the scope of EU law, can it identify the specific activity and the Union-law basis on which it is outside scope?

SOURCE VERBATIM

> 1. This Regulation does not apply to the processing of personal data:
>
> (a) in the course of an activity which falls outside the scope of Union law;
>
> — Regulation (EU) 2016/679 Article 2(2)(a), Consolidated 2016-05-04 (GDPR)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- List of processing activities the organisation claims as §2(2)(a)-excluded, if any
- Legal basis for the claim: which Union competence does the activity fall outside, and on what authority
- Confirmation from legal counsel or the relevant authority
- For processing on the boundary (e.g., contractor support to national-security work): the demarcation line and audit of activities each side of it

MANAGEMENT SYSTEM REFERENCE:

_____

FINDINGS / NOTES:

Q3 ARTICLE GDPR Art.2(2)(b)

For any processing carried out by a Member State in connection with the common foreign and security policy under TEU Title V Chapter 2, can the organisation identify the activity and confirm the exclusion was validly invoked?

SOURCE VERBATIM

> 1. This Regulation does not apply to the processing of personal data:
>
> (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
>
> — Regulation (EU) 2016/679 Article 2(2)(b), Consolidated 2016-05-04 (GDPR)

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- List of any processing claimed under §2(2)(b), if any
- Identity of the Member State authority on whose behalf the processing is carried out
- Legal basis tying the activity to a specific CFSP measure
- For private contractors supporting CFSP work: the contractual scope and the GDPR/non-GDPR demarcation

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES: