ethyx
ethyx.eu

Audit Preparation Checklist

Be ready for a GDPR supervisory-authority audit · For SMEs · EN

Reviewed by a certified Data Protection Officer (CIPP/E) · Provided by ETHYX · Version 1.0 · June 2026 · Not legal advice

HOW TO USE A supervisory authority can audit you after a complaint, a data breach, a sector-wide sweep, or at random. The best preparation is ongoing readiness: have your documentation current and accessible. Work through Sections 1–2 now so the evidence exists; use Sections 3–5 if an audit is announced. Tick each item and note where the evidence lives.

Company: _____ **Prepared by:** _____

DPO / responsible: _____ **Date:** _____

1 Documentation pack – have these ready

DONE	ITEM	WHERE IS THE EVIDENCE? / NOTES
☐	Record of Processing Activities (ROPA), current and complete. [ROPA Template]	
☐	Privacy notice(s) – website and any others – current and accurate. [Privacy Notice Template]	
☐	Data Processing Agreements (DPAs) with all processors. [DPA Template]	
☐	Technical & organisational measures documented. [TOM Checklist]	
☐	Completed DPIAs for high-risk processing. [DPIA Template]	
☐	Internal data breach register (including non-reported breaches). [Art. 33(5)]	
☐	Records of consent, where consent is the legal basis. [Art. 7(1)]	
☐	Data protection policies and procedures. [Art. 24(2)]	
☐	Staff training records. [Staff Training Tracker]	
☐	DPO appointment and contact details (if a DPO is required). [Art. 37-39]	

2 Governance & evidence of accountability

DONE	ITEM	WHERE IS THE EVIDENCE? / NOTES
☐	We can map every processing activity to a documented legal basis. [Art. 6]	
☐	Retention periods are defined and we can show deletion happens. [Art. 5(1)(e)]	

2 Governance & evidence of accountability

DONE	ITEM	WHERE IS THE EVIDENCE? / NOTES
☐	We can show how we handle data subject requests, with examples. [Art. 15-22]	
☐	International transfers have documented safeguards (SCCs/TIAs). [Art. 46]	
☐	We can demonstrate data protection by design in a recent project. [Art. 25]	
☐	Roles and responsibilities for data protection are documented. [Art. 24]	

3 Know your rights & the process

DONE	ITEM	WHERE IS THE EVIDENCE? / NOTES
☐	We understand the authority's powers (access, information requests, on-site inspection). [Art. 58]	
☐	We have identified a single point of contact to coordinate the audit.	
☐	We know our right to be informed of the scope and legal basis of the audit.	
☐	We have legal counsel / DPO contact ready to involve.	
☐	We will document all communications with the authority.	

4 During the audit – conduct

DONE	ITEM	WHERE IS THE EVIDENCE? / NOTES
☐	Respond factually and within the deadlines set by the authority. [Art. 31]	
☐	Provide only what is requested – accurate, complete, not misleading.	
☐	Keep a log of every document handed over and every question asked.	
☐	Do not destroy, alter or backdate any records.	
☐	Escalate sensitive questions to the DPO or counsel before answering.	
☐	Be cooperative and professional – cooperation is itself an obligation. [Art. 31]	

5 After the audit – follow-up

DONE	ITEM	WHERE IS THE EVIDENCE? / NOTES
☐	Obtain the authority's findings in writing.	
☐	Create a remediation plan with owners and deadlines for any gaps.	

5 After the audit – follow-up

DONE	ITEM	WHERE IS THE EVIDENCE? / NOTES
☐	Implement corrective measures and document completion.	
☐	Update the ROPA, policies and training to reflect changes.	
☐	Confirm closure with the authority where applicable.	

This checklist is provided for guidance only and does not constitute legal advice. It is based on Regulation (EU) 2016/679 (GDPR) and the German BDSG. Reviewed by a certified Data Protection Officer (CIPP/E). Provided by ETHYX – ethyx.eu. GDPR max fine: €20M / 4% of global annual turnover. Have your audit readiness reviewed by a qualified DPO or counsel. Version 1.0 · June 2026.