

TOM Checklist

Technical & Organisational Measures · Art. 32 GDPR · Template for SMEs

Reviewed by a certified Data Protection Officer (CIPP/E) · Provided by ETHYX · Version 1.1 · July 2026 · Not legal advice

HOW TO USE Work through each section and tick the box when a measure is in place. Use Status / Notes for partial status, the responsible person or the system used – write 'N/A' with a brief reason where a measure does not apply. Review at least annually. The §-numbers match the TOM references in the ETHYX ROPA template.

**Company /
controller:**

**Completed
by:**

Date:

**Next review
due:**

What this is

Article 32 GDPR requires every controller and processor to implement appropriate technical and organisational measures (TOMs) to secure personal data. This checklist documents those measures – the security annex your DPAs and ROPA refer to, and the first document an authority or enterprise client asks for.

§1 Physical access control (Zutrittskontrolle)

DONE	MEASURE	STATUS / NOTES
☐	Servers and IT equipment are kept in locked rooms with restricted access.	
☐	An access system (keys, key cards or codes) controls entry; key/card issuance is documented.	
☐	Visitors are registered and accompanied in areas where personal data is processed.	
☐	Premises are secured (alarm system, locks, and/or security service as appropriate).	
☐	A clean-desk policy applies; paper records are kept in lockable cabinets.	
☐	Paper is destroyed to DIN 66399 (shredding) and storage media are securely wiped or destroyed before disposal.	
☐	Cloud/remote setup: physical security is provided by the hosting/data-centre provider – verify their certification (e.g. ISO 27001) and record it in the DPA.	

§2

Logical access control (Zugangs- & Zugriffskontrolle)

DONE	MEASURE	STATUS / NOTES
☐	Every user has a unique personal account; shared logins are not used.	
☐	A password policy is enforced (minimum length, complexity, no reuse of compromised passwords).	
☐	Multi-factor authentication (MFA) is required for critical systems and all remote access.	
☐	Access follows least-privilege / role-based rules; an access matrix is documented and reviewed.	
☐	Screens lock automatically after inactivity; sessions time out.	
☐	Access is revoked promptly when an employee leaves or changes role (offboarding checklist).	
☐	Access to systems containing personal data is logged.	
☐	Laptops and mobile devices are managed (MDM) and encrypted.	

§3

Network & server security

DONE	MEASURE	STATUS / NOTES
☐	A firewall protects the network; segmentation separates sensitive systems.	
☐	Anti-malware protection is installed and kept current.	
☐	Patch/update management keeps operating systems and software up to date.	
☐	Systems are securely configured; unused services and default accounts are disabled.	
☐	Remote access uses a VPN or equivalent secured channel.	
☐	Security events are monitored (logging / intrusion detection as appropriate to size).	

§4

Encryption (Verschlüsselung)

DONE	MEASURE	STATUS / NOTES
☐	All data in transit is encrypted with TLS (HTTPS) – verified by the website security section.	
☐	Personal data at rest is encrypted (databases, file storage).	
☐	Full-disk encryption is enabled on all laptops and mobile devices.	
☐	Backups are encrypted.	
☐	Sensitive data sent by email is encrypted (S/MIME, PGP) or shared via a secure portal.	

§5 Pseudonymisation & anonymisation		
DONE	MEASURE	STATUS / NOTES
☐	Personal data is pseudonymised where feasible (identifiers stored separately from content).	
☐	Analytics data is anonymised (e.g. IP masking) – see the cookieless analytics setup.	
☐	Test and development environments use anonymised or synthetic data, never live personal data.	

§6 Transmission & transfer security (Weitergabekontrolle)		
DONE	MEASURE	STATUS / NOTES
☐	Data is transferred only through documented, secure channels.	
☐	A data processing agreement (Art. 28) is in place with every processor – see §11.	
☐	Files are transferred encrypted; sensitive data is never sent by unencrypted email.	
☐	Transfers of personal data to third parties are recorded.	
☐	Third-country transfers rely on a documented safeguard (e.g.	
☐	SCCs) – consistent with the ROPA.	

§7 Input control & data minimisation (Eingabekontrolle)		
DONE	MEASURE	STATUS / NOTES
☐	Audit logs record who entered, changed or deleted personal data, and when.	
☐	Logs are protected against tampering and retained for an appropriate period.	
☐	Only the personal data necessary for each purpose is collected (data minimisation).	
☐	Retention and deletion schedules are defined and applied.	

§8 Availability & resilience (Verfügbarkeit & Belastbarkeit)		
DONE	MEASURE	STATUS / NOTES
☐	Backups run regularly and automatically (following the 3-2-1 principle).	
☐	Backups are tested by periodic restore.	
☐	A disaster-recovery / business-continuity plan is documented.	
☐	Power and hardware redundancy exist where appropriate (UPS, redundant storage).	
☐	Recovery objectives (RPO/RTO) are defined.	

§9 Separation control (Trennungskontrolle)		
DONE	MEASURE	STATUS / NOTES
☐	Data is separated by purpose (logically or physically).	
☐	Production, test and development environments are separated.	
☐	In shared/multi-tenant systems, customer data is logically segregated.	

§10 Processor management (Auftragskontrolle, Art. 28)		
DONE	MEASURE	STATUS / NOTES
☐	A data processing agreement (DPA/AVV) exists with every processor.	
☐	Processors are selected for sufficient guarantees of appropriate security (Art. 28(1)).	
☐	A current list of processors is maintained – consistent with the ROPA.	
☐	Processors' security is reviewed periodically.	
☐	Sub-processors are engaged only with documented authorisation.	

§11 Data protection management & incident response		
DONE	MEASURE	STATUS / NOTES
☐	A DPO or data-protection contact is named and reachable.	
☐	A Record of Processing Activities (Art. 30) is maintained – see the ROPA template.	
☐	Staff are trained on data protection and bound to confidentiality.	
☐	A breach-response process meets the 72-hour notification duty (Art.	
☐	33).	
☐	A process handles data-subject requests within one month (Art.	
☐	15-22).	
☐	These TOMs are reviewed at least annually (Art. 32(1)(d)).	

§12 Privacy by design & by default (Art. 25)		
DONE	MEASURE	STATUS / NOTES
☐	Data protection is considered when new processes or systems are designed.	
☐	Default settings are privacy-friendly (minimal data, shortest retention).	

§12**Privacy by design & by default (Art. 25)**

DONE	MEASURE	STATUS / NOTES
☐	A DPIA is carried out where processing is high-risk (Art. 35) – see the DPIA template.	

This checklist is provided for guidance only and does not constitute legal advice. Based on Regulation (EU) 2016/679 (GDPR). Reviewed by a certified Data Protection Officer (CIPP/E). Provided by ETHYX – ethyx.eu. GDPR max fine: €20M / 4% turnover. Version 1.1 · July 2026.