

GDPR Compliance Checklist

The complete GDPR readiness checklist 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 Work through each section and tick the box when the requirement is met. Use the Status / Notes column to record gaps, owners and target dates. A ticked checklist is a snapshot, not proof of compliance – keep the underlying records (ROPA, DPAs, policies). Start with Sections 1–4; they apply to almost every business.

Company: _____

Completed by: _____

Date: _____

Next review: _____

1 Governance & accountability

DONE	REQUIREMENT	STATUS / NOTES
☐	We can demonstrate compliance with the GDPR principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity & confidentiality). [Art. 5]	
☐	A named person or role is responsible for data protection in our organisation. [Art. 24]	
☐	We have assessed whether we must appoint a Data Protection Officer (DPO). [Art. 37, §38 BDSG]	
☐	Data protection responsibilities are documented and known to staff. [Art. 24]	
☐	We have internal data protection policies (or one combined policy) in place. [Art. 24(2)]	

2 Records of processing (ROPA)

DONE	REQUIREMENT	STATUS / NOTES
☐	We maintain a Record of Processing Activities (ROPA) covering all our processing. [Art. 30]	
☐	Each entry lists purpose, legal basis, data categories, recipients, retention and TOMs. [Art. 30(1)]	
☐	The ROPA is reviewed and updated at least annually and after any new processing. [Art. 30]	
☐	We have identified all special-category data we process (health, biometrics, etc.). [Art. 9]	

3

Lawful basis & consent

DONE	REQUIREMENT	STATUS / NOTES
☐	Every processing activity has a documented legal basis (Art. 6). [Art. 6]	
☐	Where we rely on consent, it is freely given, specific, informed and unambiguous – and recorded. [Art. 7]	
☐	Individuals can withdraw consent as easily as they gave it. [Art. 7(3)]	
☐	Where we rely on legitimate interests, we have completed a balancing test (LIA). [Art. 6(1)(f)]	
☐	Special-category processing has an additional Art. 9 condition. [Art. 9(2)]	

4

Transparency & privacy notices

DONE	REQUIREMENT	STATUS / NOTES
☐	We provide a clear, accessible privacy notice to data subjects. [Art. 12-14]	
☐	The notice covers identity, purposes, legal bases, recipients, transfers, retention and rights. [Art. 13-14]	
☐	Notices are given at the point of data collection (or within one month if obtained indirectly). [Art. 14(3)]	
☐	Our website privacy notice is current and matches our actual processing. [Art. 12]	

5

Data subject rights

DONE	REQUIREMENT	STATUS / NOTES
☐	We have a documented process to handle access, rectification, erasure, restriction, portability and objection requests. [Art. 15-22]	
☐	We can respond to a request within one month (extendable by two). [Art. 12(3)]	
☐	We verify the identity of the requester before disclosing data. [Art. 12(6)]	
☐	Staff know how to recognise and escalate a data subject request. [Art. 12]	
☐	We can fulfil erasure and portability requests technically. [Art. 17, 20]	

6

Processors & contracts

DONE	REQUIREMENT	STATUS / NOTES
☐	We have a Data Processing Agreement (DPA) with every processor. [Art. 28]	

6	Processors & contracts	
DONE	REQUIREMENT	STATUS / NOTES
☐	Each DPA contains the mandatory Art. 28(3) clauses. [Art. 28(3)]	
☐	We carry out due diligence on processors' security before engaging them. [Art. 28(1)]	
☐	Sub-processors are authorised and listed. [Art. 28(2),(4)]	
7	International transfers	
DONE	REQUIREMENT	STATUS / NOTES
☐	We have identified all transfers of personal data outside the EU/EEA. [Art. 44]	
☐	Each transfer has a valid safeguard (adequacy, SCCs, BCRs or a derogation). [Art. 45-49]	
☐	Where we use SCCs, we have completed a Transfer Impact Assessment (TIA). [Art. 46]	
☐	Our privacy notice lists the third countries to which data is transferred. [Art. 13(1)(f)]	
8	Security (TOMs)	
DONE	REQUIREMENT	STATUS / NOTES
☐	We have implemented appropriate technical and organisational measures. [Art. 32]	
☐	Access to personal data is restricted on a need-to-know basis. [Art. 32(1)(b)]	
☐	Personal data is encrypted in transit and, where appropriate, at rest. [Art. 32(1)(a)]	
☐	We have documented our TOMs (e.g. via the TOM Checklist). [Art. 32]	
☐	We regularly test, assess and review the effectiveness of our measures. [Art. 32(1)(d)]	
9	Data breaches	
DONE	REQUIREMENT	STATUS / NOTES
☐	We have a documented data breach response procedure. [Art. 33-34]	
☐	Staff know how to report a suspected breach internally and quickly. [Art. 33]	
☐	We can notify the supervisory authority within 72 hours where required. [Art. 33(1)]	
☐	We maintain an internal breach register, including breaches not reported. [Art. 33(5)]	

10	DPIA & privacy by design	
DONE	REQUIREMENT	STATUS / NOTES
☐	We assess whether new processing requires a Data Protection Impact Assessment (DPIA). [Art. 35]	
☐	We apply data protection by design and by default to new projects and systems. [Art. 25]	
☐	High-risk processing without adequate mitigation triggers prior consultation. [Art. 36]	

11	Retention & deletion	
DONE	REQUIREMENT	STATUS / NOTES
☐	We have defined retention periods for each category of personal data. [Art. 5(1)(e)]	
☐	Data is deleted or anonymised when the retention period ends. [Art. 17]	
☐	Statutory retention obligations (e.g. tax, commercial law) are documented. [Art. 17(3)(b)]	

12	Training & awareness	
DONE	REQUIREMENT	STATUS / NOTES
☐	Staff who handle personal data receive data protection training. [Art. 39(1)(b)]	
☐	Training is refreshed regularly and on onboarding. [Art. 24]	
☐	We keep records of who was trained and when. [Art. 5(2)]	

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 compliance position reviewed by a qualified DPO or counsel. Version 1.0 · June 2026.