

GDPR: small-business checklist

EU / EEA | Reviewed 12 October 2026 | XnMark

Owner: _____ Review date: _____

☐ Map personal data

List collection points, purposes, recipients and storage locations.

☐ Document lawful grounds

Match each purpose to a lawful basis; review consent where used.

☐ Update privacy information

Explain your real practices clearly at the point of collection.

☐ Review suppliers and transfers

Check processor terms, sub-processors and overseas safeguards.

☐ Limit access and retention

Remove stale accounts; record retention rules and deletion checks.

☐ Test security and recovery

Check authentication, updates, backups and incident contacts.

☐ Prepare rights requests

Assign an owner and log requests; normal response: one month.

☐ Prepare breach response

Record all breaches; assess notification without delay. Where required, notify the authority within 72 hours of awareness.

Complete each item with an owner, evidence link and next action. This checklist is a starting point, not a legal certification. National marketing/cookie rules, DPIA, DPO and international-transfer requirements need a separate scope check. Sources: EDPB SME guide and European Commission GDPR application guidance. edpb.europa.eu/sme_en | commission.europa.eu/law/law-topic/data-protection Full references and scope notes: xnmark.com/insights-gdpr-checklist-eu-2026/