Venzip

DATA PRIVACY *SERIES* GUIDE

Is Your Customer Data Actually Protected?

Venzip

TABLE OF CONTENTS

Venzip

CHAPTER 1

WHY GDPR READINESS IS A BUSINESS ADVANTAGE

GDPR is not just a European regulation. It is the global benchmark for how trustworthy companies handle personal data. And your customers know it.

If your SaaS product has a single user in the EU, you are subject to GDPR. The fines are real: up to 20 million euros or 4% of global annual revenue, whichever is higher. But the bigger cost is lost trust. Enterprise buyers routinely disqualify vendors who cannot demonstrate GDPR compliance during procurement.

The companies that treat GDPR as a trust differentiator rather than a legal burden are the ones closing cross-border deals, expanding into the EU with confidence, and building the kind of data practices that customers actually want.

This guide gives you a structured, domain-based assessment of your GDPR readiness. It covers the operational requirements that auditors, DPAs, and enterprise customers actually look for, organized into 10 domains with 80+ questions and priority actions.

What makes this guide different:

- Operational focus — what you actually need to do, not legal theory
- Priority actions after each domain to turn gaps into a 90-day plan
- Board-ready summary page for presenting to leadership and investors
- Covers AI-specific GDPR requirements (automated decisions, profiling)

Venzip

HOW TO USE THIS ASSESSMENT

This assessment is organized into 10 domains covering the full scope of GDPR operational compliance. Questions are mapped to specific GDPR articles and tagged with maturity tiers.

Three Maturity Tiers

Tier 1 — Foundational

Essential for every organization processing personal data of EU residents. These are the non-negotiable requirements. Start here.

Tier 2 — Operational

For organizations with established data processing operations, multiple data processors, or customer-facing products handling personal data at scale.

Tier 3 — Advanced

For organizations conducting large-scale processing, automated decision-making, cross-border transfers, or operating in high-risk sectors like health or finance.

How to Score

1. Work through each domain. Mark Yes or No for each question.
2. Count Yes answers per domain. Review priority actions for any domain below 50%.
3. Calculate your total score and use the scoring guide on page 11.
4. Use the board-ready summary on page 12 to present findings to leadership.
5. Contact Venzip to turn your assessment into a GDPR compliance roadmap.

Key GDPR Fact

The GDPR has 99 articles and 173 recitals. You do not need to memorize them.

This guide distills the operational requirements into practical, answerable questions so you can assess readiness without a law degree.

Venzip

1. LAWFUL BASIS & CONSENT MANAGEMENT

Establishing and documenting a lawful basis for every data processing activity. Art. 6, 7, 8, 9.

TIER ID	QUESTION	YES	NO
T1 LBC-01	Have you identified and documented the lawful basis for each processing activity?	☐ YES	☐ NO
T1 LBC-02	Where consent is the lawful basis, is it freely given, specific, informed, and unambiguous?	☐ YES	☐ NO
T1 LBC-03	Can individuals withdraw consent as easily as they gave it?	☐ YES	☐ NO
T1 LBC-04	Do you have age verification mechanisms for services offered to children?	☐ YES	☐ NO
T2 LBC-05	Is legitimate interest documented with a balancing test for each applicable use case?	☐ YES	☐ NO
T2 LBC-06	Are consent records maintained with timestamps and version history?	☐ YES	☐ NO
T2 LBC-07	Do you re-obtain consent when processing purposes change materially?	☐ YES	☐ NO
T3 LBC-08	Are special category data processing activities supported by an Art. 9 condition?	☐ YES	☐ NO
T3 LBC-09	Is there a regular review cycle to validate that lawful bases remain appropriate?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Map every processing activity to a lawful basis under Art. 6
- Audit your consent flows — can users withdraw as easily as they consented?
- Document your legitimate interest assessments

DOMAIN SCORE: ___ / 9 Yes

Venzip

2. DATA SUBJECT RIGHTS

Processes for responding to individual rights requests within the required timeframes. Art. 15-22.

TIER ID	QUESTION	YES	NO
T1 DSR-10	Can you respond to subject access requests (SARs) within 30 days?	☐ YES	☐ NO
T1 DSR-11	Do you have a process for data portability requests?	☐ YES	☐ NO
T1 DSR-12	Can individuals request erasure of their personal data (right to be forgotten)?	☐ YES	☐ NO
T2 DSR-13	Is there a process to handle rectification requests when data is inaccurate?	☐ YES	☐ NO
T2 DSR-14	Can you restrict processing when requested by a data subject?	☐ YES	☐ NO
T2 DSR-15	Do you notify third parties when data is erased, rectified, or restricted?	☐ YES	☐ NO
T3 DSR-16	Is there a documented process for handling objections to processing?	☐ YES	☐ NO
T3 DSR-17	Can individuals opt out of automated decision-making and profiling?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Build a subject access request workflow with clear ownership and SLAs
- Test your erasure process end-to-end across all systems and backups

Venzip

3. PRIVACY BY DESIGN & DEFAULT

Embedding data protection into systems, products, and processes from the start. Art. 25.

TIER ID	QUESTION	YES	NO
T1 PBD-18	Is data protection considered during the design phase of new products and features?	☐ YES	☐ NO
T1 PBD-19	Are default settings configured to minimize personal data collection?	☐ YES	☐ NO
T2 PBD-20	Is personal data pseudonymized or anonymized wherever feasible?	☐ YES	☐ NO
T2 PBD-21	Do you conduct privacy reviews before launching new features that process personal data?	☐ YES	☐ NO
T2 PBD-22	Are data minimization principles applied across all processing activities?	☐ YES	☐ NO
T3 PBD-23	Is there a privacy engineering function embedded in your development process?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Add a privacy review checkpoint to your product development process
- Audit default settings in your product for data minimization

Venzip

4. RECORDS OF PROCESSING ACTIVITIES (ROPA)

Maintaining the mandatory register of all data processing activities. Art. 30.

TIER ID	QUESTION	YES	NO
T1 ROPA-24	Do you maintain a record of all processing activities as controller?	☐ YES	☐ NO
T1 ROPA-25	Does each record include purpose, data categories, recipients, and retention periods?	☐ YES	☐ NO
T2 ROPA-26	Are processing records kept up to date when activities change?	☐ YES	☐ NO
T2 ROPA-27	If you act as a processor, do you maintain a separate processor ROPA?	☐ YES	☐ NO
T2 ROPA-28	Are ROPAs available to supervisory authorities upon request?	☐ YES	☐ NO
T3 ROPA-29	Is there a defined owner responsible for maintaining the ROPA?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Create your ROPA immediately — this is a mandatory requirement for most organizations
- Assign a single owner responsible for keeping the ROPA current

Venzip

5. DATA PROTECTION IMPACT ASSESSMENTS

Conducting DPIAs for high-risk processing activities before they begin. Art. 35-36.

TIER ID	QUESTION	YES	NO
T1 DPIA-30	Do you conduct DPIAs for processing likely to result in high risk to individuals?	☐ YES	☐ NO
T1 DPIA-31	Are DPIAs completed before the processing activity begins?	☐ YES	☐ NO
T2 DPIA-32	Do DPIAs include a description of processing, necessity assessment, and risk mitigation?	☐ YES	☐ NO
T2 DPIA-33	Is there a defined threshold for when a DPIA is required?	☐ YES	☐ NO
T3 DPIA-34	Do you consult the supervisory authority when a DPIA indicates high residual risk?	☐ YES	☐ NO
T3 DPIA-35	Are DPIAs reviewed and updated when processing activities change?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Identify your highest-risk processing activity and complete a DPIA for it this quarter
- Create a DPIA template your teams can reuse for new projects

Venzip

6. THIRD-PARTY & VENDOR MANAGEMENT

Ensuring processors and sub-processors comply with GDPR through contracts and oversight. Art. 28-29.

TIER ID	QUESTION	YES	NO
T1 VEN-36	Do all data processing agreements (DPAs) include the mandatory Art. 28 clauses?	☐ YES	☐ NO
T1 VEN-37	Do you maintain a register of all data processors and sub-processors?	☐ YES	☐ NO
T2 VEN-38	Are processors required to notify you before engaging new sub-processors?	☐ YES	☐ NO
T2 VEN-39	Do you audit or assess processor compliance with GDPR obligations?	☐ YES	☐ NO
T2 VEN-40	Are processors contractually required to assist with data subject rights requests?	☐ YES	☐ NO
T3 VEN-41	Do you assess processor data breach notification capabilities before onboarding?	☐ YES	☐ NO
T3 VEN-42	Is there a process to terminate processors who fail to meet GDPR obligations?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Ensure every vendor processing personal data has a signed DPA with Art. 28 clauses
- Build a processor register listing all vendors, their purposes, and sub-processors

Venzip

7. INTERNATIONAL & CROSS-BORDER TRANSFERS

Ensuring lawful transfer of personal data outside the EEA. Art. 44-49, Chapter V.

TIER ID	QUESTION	YES	NO
T1 CBT-43	Have you identified all international transfers of personal data?	☐ YES	☐ NO
T1 CBT-44	Are transfers to countries outside the EEA supported by an adequate transfer mechanism?	☐ YES	☐ NO
T2 CBT-45	Are Standard Contractual Clauses (SCCs) in place where required?	☐ YES	☐ NO
T2 CBT-46	Have you conducted Transfer Impact Assessments (TIAs) for non-adequate countries?	☐ YES	☐ NO
T3 CBT-47	Are supplementary measures implemented where TIAs identify risk?	☐ YES	☐ NO
T3 CBT-48	Do you monitor adequacy decisions and update transfer mechanisms accordingly?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Map all data flows that cross EEA borders and identify the transfer mechanism for each
- Update your SCCs to the current EU-approved version if you have not already

Venzip

8. BREACH NOTIFICATION & INCIDENT RESPONSE

Detecting, reporting, and managing personal data breaches within GDPR timeframes. Art. 33-34.

TIER ID	QUESTION	YES	NO
T1 BIR-49	Can you detect a personal data breach and assess its severity within 24 hours?	☐ YES	☐ NO
T1 BIR-50	Is there a documented process to notify the supervisory authority within 72 hours?	☐ YES	☐ NO
T1 BIR-51	Do you have criteria for determining when affected individuals must be notified?	☐ YES	☐ NO
T2 BIR-52	Are breach notifications documented including facts, effects, and remedial actions?	☐ YES	☐ NO
T2 BIR-53	Do processors contractually commit to notifying you of breaches without undue delay?	☐ YES	☐ NO
T2 BIR-54	Is there a breach register that records all incidents regardless of notification obligation?	☐ YES	☐ NO
T3 BIR-55	Are breach response plans tested through tabletop exercises at least annually?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Draft a 72-hour breach notification procedure with clear roles and escalation paths
- Start a breach register today — even if you have had zero incidents

Venzip

9. DPO & GOVERNANCE STRUCTURE

Establishing accountability, governance, and oversight for data protection. Art. 37-39, 24.

TIER ID	QUESTION	YES	NO
T1 GOV-56	Have you assessed whether your organization is required to appoint a DPO?	☐ YES	☐ NO
T1 GOV-57	Is there a named individual or function responsible for data protection compliance?	☐ YES	☐ NO
T2 GOV-58	Does senior management demonstrate accountability for data protection?	☐ YES	☐ NO
T2 GOV-59	Are data protection policies approved by leadership and communicated to all staff?	☐ YES	☐ NO
T3 GOV-60	Does the DPO (or equivalent) have direct access to senior management?	☐ YES	☐ NO
T3 GOV-61	Is there a regular governance review of data protection policies and practices?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Assess your DPO requirement — public authorities and large-scale processors must appoint one
- Ensure your privacy lead has a direct reporting line to senior management

Venzip

10. EMPLOYEE AWARENESS & TRAINING

Ensuring all staff understand their data protection responsibilities. Art. 39(1)(b), 47(2)(n).

TIER ID	QUESTION	YES	NO
T1 TRN-62	Do all employees receive GDPR awareness training at onboarding?	☐ YES	☐ NO
T1 TRN-63	Is training refreshed at least annually?	☐ YES	☐ NO
T2 TRN-64	Are employees in high-risk roles (HR, marketing, engineering) given role-specific training?	☐ YES	☐ NO
T2 TRN-65	Is there a process to verify training completion and maintain records?	☐ YES	☐ NO
T3 TRN-66	Are contractors and temporary staff included in data protection training?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Roll out a basic GDPR awareness module for all staff within 60 days
- Include data protection in your onboarding checklist

Venzip

BONUS: AI & AUTOMATED DECISION-MAKING UNDER GDPR

VENZIP

Art. 22 gives individuals the right not to be subject to purely automated decisions with significant effects. If you use AI, these questions are critical

TIER ID	QUESTION	YES	NO
T1 AI-67	Do you inform individuals when they are subject to automated decision-making?	☐ YES	☐ NO
T1 AI-68	Can individuals request human review of automated decisions?	☐ YES	☐ NO
T2 AI-69	Are automated decisions based on special category data prohibited unless Art. 9 applies?	☐ YES	☐ NO
T2 AI-70	Do you conduct DPIAs for AI systems that process personal data?	☐ YES	☐ NO
T3 AI-71	Is there documentation of the logic, significance, and consequences of automated processing?	☐ YES	☐ NO
T3 AI-72	Do you assess AI vendors for GDPR compliance before deploying their tools?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Identify any automated decisions with legal or significant effects on individuals
- Implement a human review process for high-impact AI-driven decisions

Venzip

SCORE YOUR GDPR READINESS

Total your Yes answers across all 10 domains plus the AI bonus section. Use the guide below to understand where you stand.

60-78 Yes — Strong Posture

Mature GDPR program. Focus on continuous improvement, monitoring regulatory updates, and preparing for audits or DPA inquiries.

40-59 Yes — Developing

Solid foundation with meaningful gaps. Prioritize the domains where you scored lowest. Build a 90-day remediation plan.

20-39 Yes — Early Stage

Your GDPR program is forming. Complete all Tier 1 controls to establish a defensible baseline before advancing.

0-19 Yes — Critical Gaps

Significant compliance risk. Immediate action needed, especially on lawful basis, breach notification, and data subject rights.

YOUR TOTAL SCORE: _____ / 78

Tier 1: ___ / 26 Tier 2: ___ / 28 Tier 3: ___ / 24

GDPR Quick Reference

- Applies to: Any organization processing personal data of EU/EEA residents
- Maximum fine: €20M or 4% of global annual revenue (whichever is higher)
- Breach notification: 72 hours to supervisory authority (Art. 33)
- Data subject response: 30 days for rights requests (Art. 12)
- UK GDPR: Separate but substantially similar. Enforced by the ICO.

Venzip

BOARD-READY GDPR COMPLIANCE SUMMARY

Organization: _____

Date: _____

Assessed By: _____

GDPR Readiness by Domain

DOMAIN	SCORE	MAX	STATUS (circle)
1. Lawful Basis & Consent	___	/ 9	Good / Fair / Gap
2. Data Subject Rights	___	/ 8	Good / Fair / Gap
3. Privacy by Design & Default	___	/ 6	Good / Fair / Gap
4. Records of Processing (ROPA)	___	/ 6	Good / Fair / Gap
5. Data Protection Impact Assessments	___	/ 6	Good / Fair / Gap
6. Third-Party & Vendor Management	___	/ 7	Good / Fair / Gap
7. International & Cross-Border Transfers	___	/ 6	Good / Fair / Gap
8. Breach Notification & Incident Response	___	/ 7	Good / Fair / Gap
9. DPO & Governance Structure	___	/ 6	Good / Fair / Gap
10. Employee Awareness & Training	___	/ 5	Good / Fair / Gap
Bonus: AI & Automated Decisions	___	/ 6	Good / Fair / Gap
TOTAL	___	/ 78	OVERALL: _____

Venzip

Key Findings

1. _____
2. _____
3. _____

Recommended Next Steps

1. _____
2. _____
3. _____

Key Risks to Escalate

1. _____
2. _____

Venzip

READY TO MAKE GDPR YOUR COMPETITIVE EDGE?

Venzip helps startups and SaaS companies turn GDPR compliance from a legal burden into a trust advantage that closes deals.

What we do:

- GDPR readiness assessments with prioritized remediation roadmaps
- Privacy by Design implementation for product teams
- Data processing agreement (DPA) templates and vendor management
- Cross-border transfer mechanisms (SCCs, TIAs, adequacy mapping)
- Breach notification procedures and incident response planning
- Cross-framework compliance (GDPR + ISO 27001 + SOC 2 + AI governance)
- Board-ready privacy reporting and DPO advisory services

BOOK A FREE GDPR READINESS REVIEW

info@venzip.com
(604) 363-7138