PRIVACY AUTOMATION OPS READINESS CHECKLIST

Assess your GDPR operational maturity and find out where governance, workflows, and evidence need to improve

PRIVALEX & RESPONSUM beyond privacy

a joint assessment

EXECUTIVE SUMMARY

If a regulator or auditor asked tomorrow, could you confidently answer:

Do you have a complete, up-to-date record of every personal data processing activity in your organisation?
When did you last formally assess the risks of your highest-risk processing operations, and can you show the documentation?
If a data subject submitted an erasure request today, could you action it, log it, and evidence closure within one month?
Do you have signed Data Processing Agreements in place with every vendor that handles personal data on your behalf?
Can you show a regulator that your staff have received data protection training, not just that training was scheduled?

For many organisations, these questions are difficult to answer with certainty, not because compliance work hasn't been done, but because that work hasn't been operationalised. Policies exist. Intentions are good. But the governance decisions, workflows, and evidence trails that make compliance real and defensible are incomplete or inconsistent.

This joint assessment developed by PrivaLex and Responsum helps you identify where your organisation stands across five operational domains: governance and accountability, records and risk assessments, data subject rights, vendor management, and training and awareness.

Together, legal expertise and privacy management technology enable organisations not only to comply with the GDPR, but to demonstrate that compliance in a measurable, auditable way.

PRIVALEX

PrivaLex **provides the governance and accountability layer.** As an **external DPO** and **compliance advisory partner,** PrivaLex makes the legal and strategic decisions that underpin a defensible GDPR programme: defining legal bases, conducting genuine DPIAs and LIAs, reviewing processor contracts, designing governance models, and providing the expert oversight required by Articles 37-39. **PrivaLex ensures your compliance is structurally sound and legally defensible.**

RESPONSUM
beyond privacy

Responsum **provides the operational and technology layer.** As a privacy management platform, Responsum **operationalises compliance decisions** by turning them into s**tructured, automated workflows:** a live Record of Processing Activities linked to assessments, automated DSR deadline tracking, vendor DPA monitoring, training delivery with individual completion records, and real-time compliance dashboards. **Responsum ensures your compliance generates the evidence that proves it.**

WHY BOTH MATTER

Making the right governance decision is not enough if it is never documented. Documenting a decision is not enough if it is not maintained, monitored, or evidenced over time. **PrivaLex provides the decisions; Responsum makes them run, and makes them provable.**

HOW TO USE THIS ASSESSMENT

For each statement, select the option that best reflects your organisation's current situation.

Each answer corresponds to a score between 0 and 2:

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

Complete all five sections. Then calculate two sub-scores:

Governance Score = total of Sections I, II, and III (max 30)
Operations Score = total of Sections IV and V (max 20)

Your recommendations come from the combination of both scores, not a single total.

DISCLAIMER

This assessment provides an indicative overview based on your responses. It is for informational purposes only and does not constitute a formal compliance determination.

For a more comprehensive evaluation, contact PrivaLex for a no-obligation readiness review.

THE ASSESSMENT

I GOVERNANCE AND ACCOUNTABILITY

(Contributes to Governance Score)

Whether your organisation has defined clear ownership, documented its accountability framework, and established the governance structures required under Article 5(2) of the GDPR.

1

We have a designated Data Protection Officer or responsible person with formally defined authority and independence from operational management.

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

2

Accountability for data protection decisions is formally assigned across departments, not held informally by a single person.

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

3

Our governance model (roles, escalation paths, decision rights) is documented and reviewed at least annually.

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

4

Privacy by design is formally considered and recorded when launching new products, processes, or systems.

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

5

We conduct a structured annual review of our overall GDPR compliance programme and document the findings.

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

II RECORDS AND RISK ASSESSMENTS

(Contributes to Governance Score)

Whether your Record of Processing Activities reflects your actual operations, and whether required risk assessments are methodologically sound, documented, and kept current in accordance with Articles 30 and 35.

6 **Our Record of Processing Activities is complete, accurate, and reflects what we actually do, not what we planned to do when we first documented it.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

7 **Every processing activity in our RoPA has a documented legal basis, with a rationale for why that basis applies to that specific activity.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

8 **We have conducted DPIAs for all processing activities that are likely high risk, not only those that are obviously high risk.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

9 **Where we rely on legitimate interests, we have a documented Legitimate Interests Assessment that a regulator could review.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

10 **Our assessments are reviewed and updated when the underlying processing activity, system, or risk changes, they are not left static after initial completion.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

III TRAINING AND AWARENESS

(Contributes to Governance Score)

Whether data protection training is correctly designed, delivered to the right people, evidenced at the individual level, and, for organisations in Spain, structured to qualify for FUNDAE public funding.

11 **All staff with access to personal data receive data protection training before they handle personal data independently, not only at annual review cycles.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

12 **Training content is reviewed and updated when regulations, internal processes, or risk profiles change, it is not static material delivered repeatedly without revision.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

13 **Staff with heightened data protection responsibilities, DPO function, IT, HR, legal, and marketing, receive role-specific training beyond general staff awareness.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

14 **Training completion is tracked per individual and we hold documented proof of completion that could be produced to a regulator, auditor, or certification body on request, without manual reconstruction.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

15 **Our training programme is structured and documented in a way that qualifies for FUNDAE public funding (in Spain), or we have formally assessed whether it could, and if not, we understand why.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

IV DATA SUBJECT RIGHTS

(Contributes to Operations Score)

Whether your organisation can receive, action, track, and evidence responses to data subject requests within the timeframes required by Articles 12–22.

16 **We have a defined intake process for receiving data subject requests across all channels, email, web form, phone, and in-person.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

17 **Every data subject request is logged from the moment of receipt, with timestamps, assigned ownership, and a tracked deadline.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

18 **We can consistently meet the one-month response deadline under Article 12, including when requests are complex or volumes are high.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

19 **We have a documented and tested process for erasure requests, including how we verify identity, action the request, and log the outcome.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

20 **We retain a complete record of every DSR, including requests we refused, the reasons given, and any communications sent to the data subject.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

V VENDOR MANAGEMENT

(Contributes to Operations Score)

Whether your organisation has identified all processors handling personal data on your behalf, and whether Article 28 obligations are being met in practice, not just at the point of contract signing.

21 **We have a complete inventory of every third-party vendor that processes personal data on our behalf.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

22 **Every vendor acting as a data processor has a signed, current Data Processing Agreement that meets Article 28 requirements.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

23 **We assess the data protection practices of new vendors before engagement, not after they already have access to personal data.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

24 **We monitor sub-processor changes notified by our vendors and assess their impact before accepting them.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

25 **We periodically review our vendor inventory and DPA status, it is not a document completed at onboarding and never revisited.**

0

0 - Not implemented or unknown
1 - Partially implemented or inconsistently applied
2 - Fully implemented, documented, and maintained

SCORING AND INTERPRETATION

Calculate your Governance Score
Add your scores from Sections I, II, and III. Maximum: 30.

0

Score	Label
0 - 10	Foundational gaps
11 - 20	Structural gaps
21 - 30	Solid foundation

Calculate your Operations Score
Add your scores from Sections IV, and V. Maximum: 20.

0

Score	Label
0 - 7	Foundational gaps
8 - 14	Partial implementation
15 - 20	Functioning operations

Find your recommendation on the following pages.
Your result is the combination of both scores.

RESULTS AND RECOMMENDATIONS

Governance: Foundational gaps (0 - 10) + Operations: Foundational gaps (0 - 7)

What your scores indicate:
Your compliance programme needs to be built from the ground up. Governance structures, legal bases, and risk assessments are absent or unreliable. Data subject rights handling and vendor oversight do not yet operate as formal, evidenced processes.

At this stage, attempting to automate compliance operations before the governance layer exists will produce a system that runs the wrong things efficiently.

Your priority:
Start with PrivaLex. A structured compliance maturity assessment will establish what your programme needs to include, define your legal bases and governance model, design your training programme, and produce a prioritised remediation plan.

Once that foundation is in place, Responsum provides the operational infrastructure to run it, DSR workflows, vendor register, and compliance dashboards, so that what PrivaLex designs, Responsum operates and evidences.

Recommended next step:
Contact PrivaLex for a compliance programme design engagement.
Responsum onboarding follows as part of implementation.

RESULTS AND RECOMMENDATIONS

Governance: Foundational gaps (0 - 10) + Operations: Partial implementation (8 - 14)

What your scores indicate:
Some operational processes are running, you are handling DSRs and managing vendors to a degree, but the governance layer underneath them is weak. Legal bases may not be correctly assigned. Risk assessments may be absent or methodologically unsound.

The operational work being done may not be legally defensible because the decisions it depends on have not been properly made.

Your priority:
PrivaLex first. The risk here is not that you are doing nothing, it is that you are doing things that may not withstand regulatory scrutiny because the legal foundations are incorrect.

PrivaLex will review and correct your governance model, legal bases, risk assessments, and training programme. Once the governance layer is sound, Responsum can be configured to close the remaining operational gaps and generate a complete evidence trail.

Recommended next step:
Contact PrivaLex for a governance and legal bases review.
Targeted Responsum configuration follows to close operational gaps.

RESULTS AND RECOMMENDATIONS

Governance: Foundational gaps (0 - 10) + Operations: Functioning (15 - 20)

What your scores indicate:
This is an unusual but important profile. Your operational processes are well-run, DSRs are tracked, vendors are managed, evidence is being generated. But the governance foundations underneath those operations are weak.

You are running compliance efficiently without being certain that what you are running is legally correct. This creates a specific risk: a well-documented programme built on incorrect legal bases or absent risk assessments is not a defensible programme.

Your priority:
PrivaLex exclusively, at least initially. The operational layer is working, the urgent need is to validate and correct the governance and legal basis layer before the gap is exposed in an audit or regulatory inquiry.

PrivaLex will conduct a governance review, correct legal bases, commission any missing assessments, and design a training programme that reflects your actual obligations. Responsum requires little intervention at this stage beyond connecting existing operations to a corrected governance framework.

Recommended next step:
Contact PrivaLex for a governance audit and legal bases review.

RESULTS AND RECOMMENDATIONS

Governance: Structural gaps (11 - 20) + Operations: Foundational gaps (0 - 7)

What your scores indicate:
Your governance structures exist but are incomplete or not fully embedded. Meanwhile, the operational processes for running compliance day-to-day are significantly underdeveloped. You have foundations to build on but the practical machinery, DSR handling, vendor oversight, training evidence, is missing or unreliable.

The risk is that governance decisions are being made but not operationalised, so they produce no evidence and cannot be demonstrated.

Your priority:
Run both work streams in parallel. PrivaLex should address the structural governance gaps, particularly assessments that are absent, legally weak, or outdated, and training programmes that are not producing documentable proof of completion. Simultaneously, Responsum should be deployed to build the operational infrastructure: DSR workflows with full audit trails, a maintained vendor register, and compliance dashboards that give ongoing visibility.

Both layers can develop together at this stage without one blocking the other.

Recommended next step:
Contact PrivaLex for a targeted assessment and training review.
Begin Responsum deployment in parallel.

RESULTS AND RECOMMENDATIONS

Governance: Structural gaps (11 - 20) + Operations: Partial implementation (08 - 14)

What your scores indicate:
This is the most common profile for organisations that have invested in compliance but have not fully closed the loop between governance decisions and operational evidence. Some things work well. Others depend on manual effort, individual knowledge, or documentation that has not been maintained.

The gap is not between doing compliance and doing nothing, it is between doing compliance and being able to demonstrate it consistently.

Your priority:
Both, with defined focus areas. PrivaLex should address the specific governance gaps, typically outdated or methodologically weak assessments, incomplete legal basis documentation, training that is delivered but not formally evidenced, or governance roles that exist on paper but not in practice. Responsum should replace manual operational processes with automated workflows and generate the evidence trail that makes existing work defensible, particularly for DSR handling and vendor management.

This combination typically produces the fastest visible improvement in overall compliance posture.

Recommended next step:
Contact PrivaLex for targeted governance remediation.
Configure Responsum to automate DSR and vendor workflows and close evidence gaps.

RESULTS AND RECOMMENDATIONS

Governance: Structural gaps (11 - 20) + Operations: Functioning (15 - 20)

What your scores indicate:
Your operational processes are working well and generating evidence. The remaining gaps are in the governance layer, assessments that need updating, legal bases that need reviewing, or training that needs to be formalised and better evidenced.

You are close to a fully defensible programme; the outstanding work is primarily on the legal and structural side.

Your priority:
PrivaLex, with a focused scope. The operational layer needs little intervention. PrivaLex should conduct a targeted review of your governance and assessment quality, ensure your training programme reflects current obligations and produces documentable proof of completion, and identify any legal basis or DPIA gaps.

If formal certification, such as ISO 27701, is on your horizon, this is also the right moment to begin that conversation.

Recommended next step:
Contact PrivaLex for a governance quality review and, if relevant, a certification readiness assessment.

RESULTS AND RECOMMENDATIONS

Governance: Solid foundation (21 - 30) + Operations: Foundational gaps (0 - 7)

What your scores indicate:
Your governance is sound. Legal bases are documented, assessments are methodologically defensible, your training programme is structured and evidenced, and your compliance programme is legally correct.

The gap is entirely operational: the frameworks and decisions that PrivaLex-level work has produced are not yet running as day-to-day workflows, and they are not generating the operational evidence that makes compliance demonstrable under scrutiny.

Your priority:
Responsum. The governance work is done, now it needs to be operationalised. Responsum translates your governance framework into live workflows: a maintained RoPA linked to assessments, DSR tracking with a complete audit trail, a vendor register that monitors DPA status and sub-processor changes, and compliance dashboards that give real-time visibility into your posture.

PrivaLex may be useful for periodic advisory, but the immediate and primary engagement is operational.

Recommended next step:
Begin Responsum deployment and configuration.
PrivaLex moves to a periodic advisory role.

RESULTS AND RECOMMENDATIONS

Governance: Solid foundation (21 - 30) + Operations: Partial implementation (8 - 14)

What your scores indicate:
Your governance foundations are strong and your operations are partially in place. The gap is in the consistency and evidence quality of your day-to-day compliance processes. DSRs may be handled but not fully logged. Vendors may be managed but the register is not actively maintained.

The compliance work is real, it just does not yet generate the evidence trail needed to demonstrate it on demand.

Your priority:
Responsum, with targeted focus. Deploy or optimise Responsum's DSR module to close audit trail gaps, activate the vendor management module to maintain a live register with DPA status tracking, and use compliance dashboards to identify and address recurring gaps proactively.

PrivaLex is not the priority here, though periodic advisory may be valuable for reviewing assessment currency and preparing for certification.

Recommended next step:
Optimise your Responsum configuration to close operational evidence gaps.
Schedule a periodic PrivaLex review to maintain governance quality.

RESULTS AND RECOMMENDATIONS

Governance: Solid foundation (21 - 30) + Operations: Functioning (15 - 20)

What your scores indicate:
Your programme is mature. Governance is sound, operations are running, and evidence is being generated across all five domains.

The question at this stage is not whether your compliance is real, it is whether it is optimised, scalable, and positioned to withstand increasing scrutiny as your organisation grows and as regulatory expectations evolve.

Your priority:
Optimisation and strategic development. Use Responsum dashboards to identify recurring gaps or overdue actions that indicate underlying process weaknesses. Commission PrivaLex to assess emerging risk areas, AI systems, new international data transfers, expanded processing activities, before they become unmanaged obligations.

If formal certification is not yet in place, this is the right moment: PrivaLex supports the full certification journey across ISO 27701, ISO 42001, and related frameworks, with a 100% client success rate. If you operate in Spain, ensure your training programme is fully optimised for FUNDAE funding.

Recommended next step:
Contact PrivaLex for advanced advisory and certification planning.
Review Responsum dashboards for optimisation opportunities.

PRIVALEX BENEFITS

Governance that holds under scrutiny.
PrivaLex translates GDPR obligations into structured, legally sound processes, not just policy documents. Compliance is built on correct legal bases, genuine risk assessments, and formal governance decisions.

Reduced audit and regulatory exposure.
Structured risk assessments, DPIAs, and DPO oversight mean your organisation can respond to regulatory inquiries and audits from a position of demonstrable control rather than reactive reconstruction.

Expert DPO function without headcount.
PrivaLex's external DPO service provides independence, regulatory knowledge, and continuity, all required under Article 37, without the cost of a full-time hire.

Clear prioritisation of compliance risk.
By assessing your programme against GDPR requirements and relevant frameworks, PrivaLex helps leadership teams focus resources on what actually matters most.

RESPONSUM BENEFITS

A living compliance programme, not a static one.
Responsum keeps your RoPA, assessments, vendor register, and training records current, automatically triggered, tracked, and evidenced as your organisation evolves.

Evidence on demand.
Every decision, assessment, DSR action, and training completion is logged with timestamps, approvals, and change history, ready to produce in response to a regulator, auditor, or data subject at any time.

Automated workflows that reduce manual burden.
DSR deadlines, DPIA triggers, vendor review cycles, and training reminders are managed by the platform, not by calendar alerts and spreadsheets.

Dashboards that show compliance posture in real time.
Leadership and DPOs get continuous visibility into open gaps, overdue actions, and overall compliance health, not a once-a-year snapshot.

WHAT'S NEXT?

At PrivaLex and Responsum, we help organisations **move from compliance as a project to compliance as an operation,** governed by expertise, run by technology, and evidenced continuously.

Based on your results, your next step may involve establishing or strengthening the governance layer, operationalising workflows and evidence trails, or aligning both under a structured improvement roadmap.

PrivaLex: External DPO services, GDPR advisory, risk assessments, and certifications.

Responsum: Privacy management platform: RoPA, DPIAs, DSR workflows, vendor management, training, and dashboards.

GET IN TOUCH

Don't wait for a regulatory request, a data subject complaint, or an audit to test your readiness.

PRIVALEX & RESPONSUM beyond privacy