GRC+ SERVICE SHEET · NOVEMBER 2026

Data Protection Compliance Audit

The GDPR makes you accountable: you must be able to show that your processing complies, review your measures and test the security of your data. We audit how your privacy programme works in practice, on real records, requests and contracts, and give you a report your management, clients and supervisory authority can rely on.

SERVICE	USUALLY TAKES
Advisory service	**Weeks, usually, from kick-off to the audit report**

What It Is

An independent audit of how your organisation meets its data protection law in practice: records, legal bases, rights, security, processors, trackers and breaches, tested on real cases.

WHY IT MATTERS

Policies on paper do not prove compliance

Supervisory authorities, clients and auditors ask for evidence that the programme works, not only that it exists.

- Records drift away from real processing
- Requests and breaches handled differently across teams
- Processor contracts and transfers not kept up to date

THE OUTCOME

Evidence you can show

Your DPO and management know where you stand, and you can answer authorities and clients with an independent report.

- A report for management and the DPO
- Priorities that reduce the most risk
- Input for your yearly privacy plan

What We Audit

Records and legal bases	Your records of processing against what really happens, and the legal basis and notice for each purpose.
Rights and requests	How access, erasure and objection requests are handled, timed and documented, on a sample of real cases.
Processors, transfers and security	Article 28 contracts, transfer safeguards and the technical and organisational measures that protect the data.
Each finding with a recommendation	Every gap comes with its risk, the GDPR article it concerns and a practical recommendation.

What You Receive

The audit report PDF	Scope, method and a conclusion for each area, with the evidence behind it.
Findings and recommendations Excel finding list	Each gap with its risk, the article concerned and a practical recommendation.
A privacy roadmap One-page plan	What to fix first, and what can wait for the next yearly cycle.
A management summary Presentation and a closing call	The result and the decisions needed, presented to management and the DPO.

From Scoping to Audit Report

1	**Scoping** Entities, processes and systems in scope, and the samples we will test.
2	**Documents** Records of processing, notices, policies, contracts and incident logs.
3	**Interviews and sampling** Short sessions with process owners and tests on real requests, contracts and processing.
4	**Draft findings** You see every conclusion before it is final and can add evidence.
5	**Audit report** The report and a management summary.

A guide, not a fixed promise: the length of each phase depends on your scope and on how quickly evidence and people are available.

Regulations That Ask for It

GDPR	An independent audit of how your organisation meets its data protection law in practice: records, legal bases, rights, security, processors, trackers and breaches, tested on real cases.
NN 14/2019 (Croatia)	A review of how your health data processing meets Articles 19, 31 and 32 alongside the GDPR.
Dz.U. 2020 poz. 666 (Poland)	A review of your medical records security against § 1 and the GDPR.
PDPA (Singapore)	An independent audit of how you meet your data protection law in practice, tested on real records and requests.
PDPL (Saudi Arabia)	
PIPEDA (Canada)	
PDPO (Hong Kong)	
PDPL (UAE)	
PDPL (Bahrain)	
PDPPL (Qatar)	
UK GDPR (United Kingdom)	
FADP (Switzerland)	

Why Organisations Choose GRC+ for Data Protection Audits

Privacy and audit expertise together	Audits are led by an auditor who holds the CIPP/E privacy and CISA audit certifications.
Tested on real cases	We sample actual requests, contracts and processing, so the report shows how the programme works.
Independent of your DPO	The audit gives your DPO an independent view to report on.
One audit, more frameworks	Our mappings link privacy laws to ISO 27701 and ISO 27001, so the evidence serves those audits too.

Questions Buyers Ask

Our DPO already checks compliance. Why an audit?

The DPO monitors compliance, but cannot independently audit the programme they help run. An audit gives management and the board an independent view.

Do you test real cases?

Yes. Every audit tests a sample of data subject requests, breaches and processor contracts, not only the policies.

Will the report be shared with the regulator?

Only if you decide so. The report is yours, written so a regulator could follow it if you ever need to show it.

Does the GDPR require an audit?

Not by name, but you must be able to demonstrate compliance (Article 5(2)), review your measures (Article 24) and regularly test the security of processing (Article 32). An independent audit is the most direct way to show all three.

Talk to Us

Tell us your role, the entities in scope and what prompts the audit. We send a written proposal with scope, dates and a fixed fee.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/gdpr-compliance-audit

