

The Data Privacy Chronicle

Edition # 2 – It is time for your annual data privacy compliance audit: key points to (re)check

The Data Privacy Chronicle is a sequence of pragmatic newsletters mainly designed for Data Protection Officer (“DPOs”), privacy leaders and their respective organisations. The aim is simple: to provide you with practical insights, powered by our experience as data protection lawyers and DPO-as-a-Service providers, on emerging topics that shape your role and to help you navigate the growing complexity of regulatory frameworks in the digital era.

Our first edition tackled a very “trendy” topic: [AI Governance and the DPO’s role](#).

This new edition covers another important and timely topic: **the annual data privacy compliance audit**.

1. Introduction

As the end of the year approaches, it is the perfect time for DPOs and privacy teams to take a step back and reflect.

Beyond budgets and strategic planning, the annual data privacy compliance audit is an opportunity to assess where your organisation stands in terms of compliance, identify areas for improvement, and prepare for what lies ahead.

The regulatory landscape has continued to evolve throughout 2025, with new enforcement trends, increased scrutiny on accountability and international transfers, and growing expectations on AI governance, data security and the recent draft Digital Omnibus Package proposed by the European Commission on 19 November 2025. These developments have reinforced one key message: privacy compliance is definitely an ongoing exercise.

A structured annual review allows the DPO and the organisation to anticipate regulatory risks, ensure documentation remains up to date, and confirm that day-to-day practices still align with both the GDPR and sector-specific rules. More importantly, it helps to demonstrate, in practice, the principle of accountability which is central in data protection.

2. Annual data privacy compliance audit: where to start?

An effective annual audit is not about ticking boxes. It is about understanding whether your organisation's privacy framework (still) works in reality, not only on paper.

Start by revisiting the core compliance pillars: governance, documentation, security, and culture. From there, the DPO and privacy teams can identify focus areas and prioritise actions for the coming year.

Below are a few examples of key questions that typically guide such an audit:

- **Governance and roles:** Are responsibilities clearly defined and up to date? Has your organisation experienced structural changes (new entities, mergers, acquisitions) that should be reflected in your privacy governance?
- **Records and documentation:** Is your Record of Processing Activities ("**ROPA**") still accurate? Are your policies, notices and data protection impact assessments ("**DPIAs**") properly reviewed and versioned?
- **Data subject rights:** Are the procedures for handling data subject requests still efficient and documented? Have deadlines been respected in practice?
- **Security and incident management:** Has your organisation updated its security measures to match evolving threats? Have potential data breaches been properly logged and reviewed?
- **Third-party management:** Are data processing agreements and vendor due diligence processes still aligned with reality, especially when new service providers have been onboarded during the year?
- **International transfers:** Are transfer mechanisms still valid following legal and regulatory updates and assessments properly done?

Of course, the specific scope of your audit will depend on your organisation's risk profile and business model. For some entities, sectoral rules (banking, insurance, healthcare) or the use of new technologies (AI tools, monitoring systems, cross-border data flows) may require additional controls.

3. Key challenges identified during annual data privacy compliance audits

Annual audits often highlight structural gaps, blind spots, or inconsistencies that progressively weaken an organisation's compliance posture. In our experience, the biggest challenges are often less about the law itself and more about how privacy governance operates in practice.

For instance, organisations frequently struggle with documentation updates: policies, ROPA or DPIAs that once reflected reality but no longer match current practices, systems or data flows. This is particularly common in fast-growing companies or environments where tools and processes evolve quickly.

Another recurring challenge is third-party oversight. Vendors are added throughout the year, cloud services change, AI features appear in tools that did not previously include them, and yet the associated checks (due diligence, contracts, transfer safeguards) are not always updated accordingly.

We also observe inconsistent involvement of the DPO / privacy team. While the GDPR expects the DPO / privacy team to be consulted "*in a timely manner*", they often learn about projects well after they are launched, making it more difficult to correct design flaws or assess risks effectively.

Finally, many organisations continue to face practical issues with data subject rights handling: response timings, identification challenges, unclear internal responsibilities, or technical limitations that make it difficult to fully honour requests. These are manageable problems, but if left unattended, they can lead to unnecessary regulatory exposure and potential sanctions.

Focus: practical steps and common pitfalls

The following tips, inspired by our experience, can help structure your approach (non-exhaustive list):

1. **Use your audit as a strategic tool.** Go beyond compliance and identify areas that can create value, greater operational efficiency and reduced risk exposure.
2. **Leverage your metrics.** Statistics on data subject requests, incidents, DPIAs, or training completion rates can reveal weak spots or trends worth addressing in 2026.
3. **Review your documentation.** Ensure that what's written reflects reality (in particular regarding your ROPAs, DPIAs, etc).
4. **Engage with key stakeholders.** The audit is not just about policies; it is also about culture. Checking how your different teams handle privacy in their day-to-day operations can be as valuable as any document review.

5. Plan for the next year. Identify priority actions, assign ownership, and schedule follow-up reviews. Documentation of these plans demonstrates continuous improvement which will be key in terms of accountability.

4. Recommendations for organisations and their DPOs / privacy leaders

So how can organisations and DPOs move from identifying risks to actively managing them?

A good annual audit does not end with a list of observations. Instead, it should be turned into a roadmap. Below are some key recommendations.

- **Prioritise what matters most**

Not all findings require the same level of investment. Focus on what creates legal risk based on your organisation, sector and the type of data processed and define a step-by-step remediation plan.

- **Refresh your documentation ecosystem**

The end of the year is the ideal moment to ensure your documentation reflects reality. Even small inconsistencies, outdated notices, missing processing purposes, or policies that do not match current tools, can undermine your organisation's accountability.

- **Reassess your vendor and transfer landscape**

Vendors evolve, new sub-processors are added, and jurisdictions change their legislation. A high-level review allows you to anticipate contractual updates, transfer impact assessments reviews, or contractual renegotiations that may be required in 2026.

- **Reinforce privacy culture internally**

Consent and training fatigue is real, but awareness remains the strongest safeguard against incidents. Tailored advice, dynamic workshops and/or updates for your colleagues with new tools or responsibilities can significantly improve compliance in practice.

- **Plan the year ahead**

Use the audit outcomes to define your privacy roadmap: priorities, timelines, responsibilities, and required resources. This proactive approach also demonstrates maturity to management and regulators.

By following these steps, DPOs can help their organisations embrace AI responsibly, while protecting individuals' rights and reducing regulatory and reputational risks.

5. Conclusion

The end of the year provides DPOs/ privacy teams with a unique window to step back, reflect and prepare for the year ahead. A well-structured annual audit is both a compliance exercise and a strategic opportunity: it shows maturity, builds trust with management and regulators, and strengthens internal awareness.

In an environment where enforcement is getting stricter and regulatory expectations continue to evolve, organisations and DPOs who approach their annual audit proactively will be best positioned to navigate the future with confidence.

HOW WE CAN HELP

At **Stellan Partners**, our Technologies, Data & IP team assists clients in navigating these challenges by:

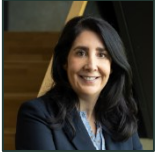
- Conducting or supporting **annual DPO audits** and compliance reviews;
- Assisting in the **update of key documents** (ROPA, DPIAs, privacy policies, international transfer tools);
- Providing **training sessions and workshops** to raise awareness and strengthen data protection culture;
- Offering **tailored checklists and audit frameworks** adapted to your sector and risk profile.

Please contact the members of our Technologies, Data & IP team should you need any assistance.

STELLAN PARTNERS

LAW FIRM

NEWSLETTER



Audrey Rustichelli

Deputy Managing Partner

New Technologies, Data & IP

audrey.rustichelli@stellanpartners.lu

T: +352 661 463 238

This newsletter has been prepared by Stellan Partners for general guidance only. Although the greatest care has been taken to ensure that the information contained therein are accurate on the date of publication, Stellan Partners does not accept any liability to any person for the information (or the use or reliance upon such information) which is provided in this handbook or incorporated into it by reference. On any specific matter, please contact us for appropriate advice. The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination, or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from any computer.

Stellan Partners, SARL, Société d'avocats inscrite au Barreau de Luxembourg

13, rue Jean Fischbach, L-3372 Leudelange / T : +352 26 48 42 1 F : +352 26 48 42 35 00 E : info@stellanpartners.lu – <https://stellanpartners.lu/>

TVA: No. Lu 25463506 – R.C.S. Luxembourg B 169476

©2025 Stellan Partners, SARL. All rights reserved.