How to Achieve GDPR Compliance Efficiently and Cost-Effectively

For business leaders and compliance professionals who are tired of wasting resources.

Melodie Lange Privacy & Security Consulting

CONTENTS

COPYRIGHT

This publication is designed to provide accurate and authoritative information regarding the subject matter covered. It is not intended as legal advice or as a professional service in any way. If you require expert assistance, seek the services of a competent professional.

Design and cover art by Rizwan Shafique.

Disclaimer: The author makes no guarantees to the results you will achieve reading this whitepaper. Results vary based on the work invested and the expertise of the persons involved.

EXECUTIVE SUMMARY

GDPR compliance is not a one-time endeavor but a continuous process that requires ongoing updates and improvements.

Since its enforcement in 2018, navigating the General Data Protection Regulation (GDPR) remains a challenge for companies of all sizes, particularly smaller companies with limited resources.

This whitepaper addresses a core issue: the absence of a structured implementation strategy, resulting in non-compliance, inefficient resource use, and struggles with evolving privacy regulations.

The methodology outlined advocates a strategic approach to GDPR compliance, sequencing tasks to optimize resource use and ensure comprehensive compliance.

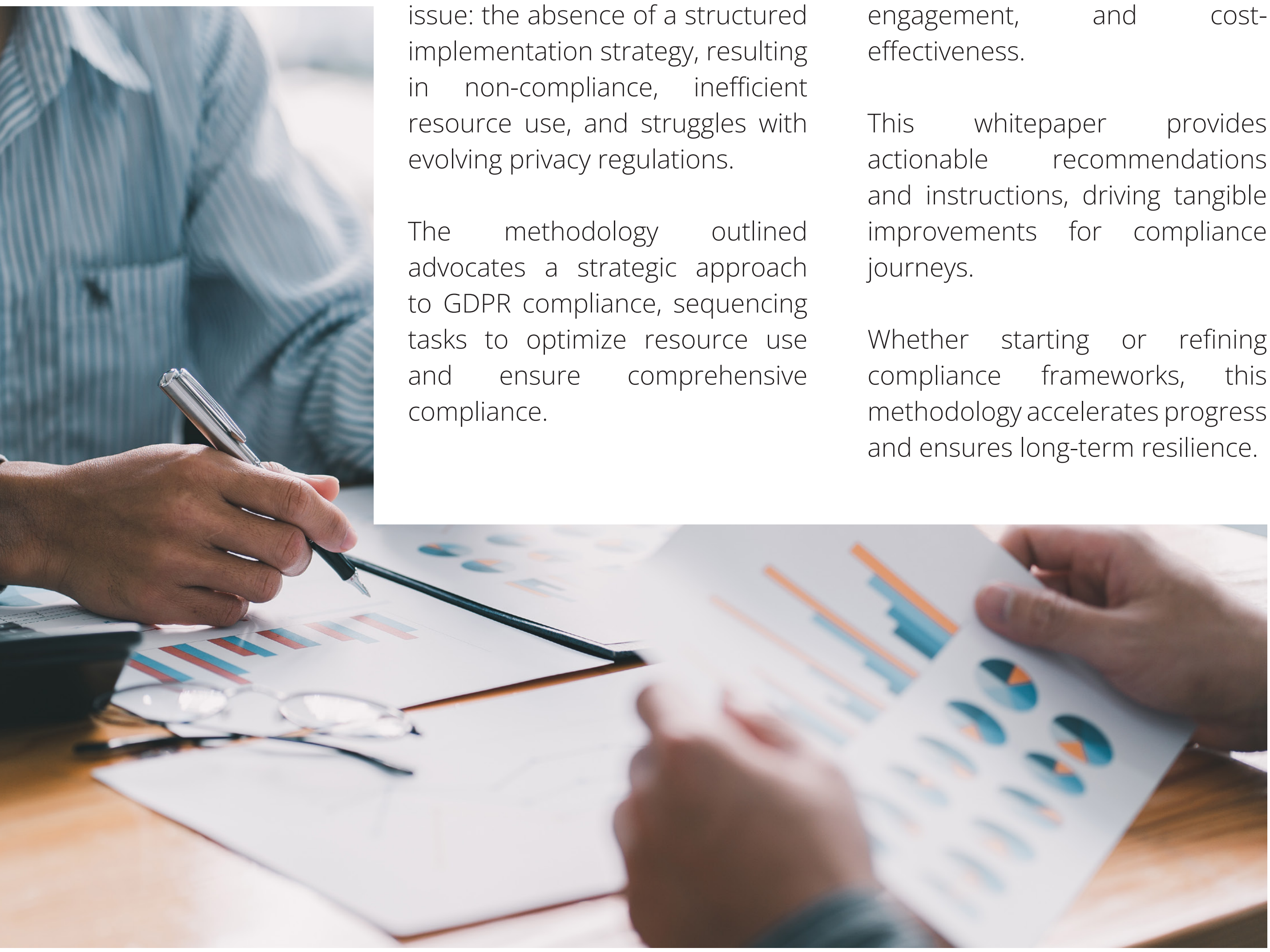
By leveraging completed tasks and existing documentation, companies can streamline compliance efforts.

This methodology offers an alternative for companies facing challenges and seeking different outcomes.

Embracing a strategic approach enhances compliance levels, operational efficiency, employee engagement, and cost-effectiveness.

This whitepaper provides actionable recommendations and instructions, driving tangible improvements for compliance journeys.

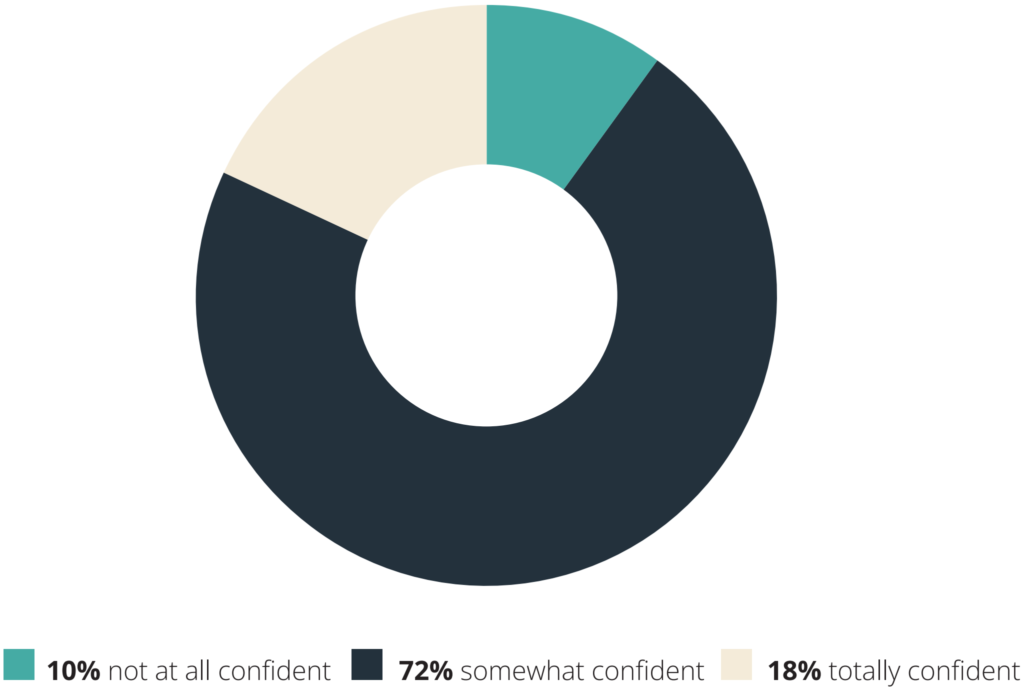
Whether starting or refining compliance frameworks, this methodology accelerates progress and ensures long-term resilience.



THE PERSISTENT STRUGGLE WITH GDPR COMPLIANCE

Since the General Data Protection Regulation (GDPR) was enforced in 2018, numerous companies are still working on their initial to-do list.

In a recent comprehensive report[1] only 2 out of 10 surveyed companies were completely confident in their organization's compliance with privacy.



Besides confusion about GDPR requirements or how to implement them properly, the lack of human resources significantly hinders compliance progress. The latter is often a result of limited budgets.

Understandably, companies hesitate to invest money in work that does not directly translate to making more profits. Yet, according to the report, 41% of the surveyed companies agree, and 22% even strongly agree that the lack of resources limited their abilities to deliver on objectives.[2]

[1] IAPP-EY Privacy Governance Report 2023, p. 9, https://iapp.org/resources/article/privacy-governance-full-report/
[2] IAPP-EY Privacy Governance Report 2023, p. 42, https://iapp.org/resources/article/privacy-governance-full-report/

> With limited human resources and budgets, every GDPR compliance effort must be strategic and effective to deliver meaningful results.

However, according to this report, many companies don’t have a strategic approach to GDPR implementation.

Instead, they “operate in a more reactive than proactive manner and may be less able to anticipate issues ... Privacy pros working in organizations that do not have a privacy strategy may therefore need to consider whether their time, resources and budgets are effectively focused.”[3]

With new privacy laws emerging, companies are further overwhelmed and need help determining where to direct their focus.

This whitepaper serves a crucial purpose: to provide clarity and offer a strategic approach to a achieve and maintain GDPR compliance in the most resource efficient way.

[3] IAPP-EY Privacy Governance Report 2023, p. 19, https://iapp.org/resources/article/privacy-governance-full-report/

INEFFECTIVE APPROACHES TO GDPR COMPLIANCE

Companies have adopted various common approaches to handle GDPR compliance However, these methods often prove to be inefficient, risky, and costly.

Common Approaches to GDPR Compliance

01

Ignoring the Issue

Ignoring GDPR compliance, hoping that non-compliance will not result in any consequences.

02

Reactive Compliance

Addressing GDPR issues only when audits, concerns, leadership directives or external urgencies like breaches, data subject requests, or media attention demand immediate action.

03

Random Compliance Efforts

Implementing GDPR compliance measures sporadically without a coherent plan or when they become urgent.

The Drawbacks

Unstrategic GDPR implementation leads to inefficiencies and heightened risks and incurs significant financial costs. Here's how these challenges manifest across three critical areas.

Time

Ignoring GDPR compliance or implementing sporadic measures without a coherent plan leads to inefficiencies, delays progress, and prolongs non-compliance.

Additionally, last-minute fixes during crises, like data breaches, disrupt operations, divert attention from core activities, and reduce overall productivity.

Risk

Failing to comply with GDPR systematically exposes businesses to substantial risks, increasing the likelihood of fines, data breaches, or subsequent legal actions.

Non-compliance can potentially damage a company's reputation, affecting customer trust and loyalty, leading to a loss of business and a competitive disadvantage.

Money

Poor GDPR compliance practices can lead to significant financial impacts from fines, legal actions, and reputational damage.

Additionally, the high cost of reactive compliance efforts is often overlooked, as urgent, last-minute fixes require more resources than proactive planning.

Conclusion

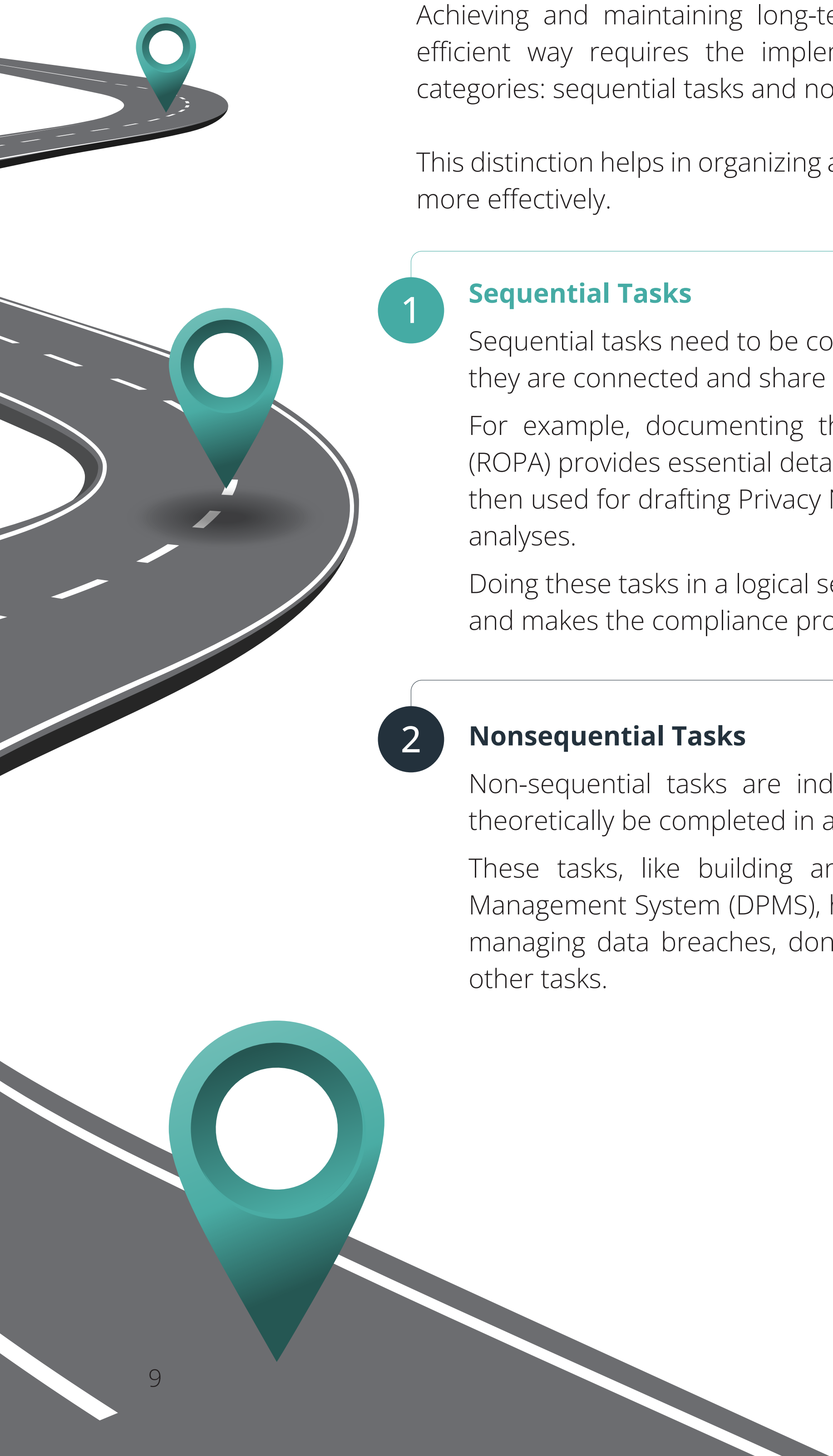
To avoid these pitfalls, businesses must adopt a strategic and proactive approach to GDPR compliance, ensuring that their efforts are efficient, well-coordinated, and cost-effective.

THE RESOURCE SAVING GDPR ROADMAP

Identifying GDPR Tasks

Achieving and maintaining long-term GDPR compliance in a resource efficient way requires the implementation of the following two task categories: sequential tasks and non-sequential tasks.

This distinction helps in organizing and prioritizing the compliance process more effectively.



1

Sequential Tasks

Sequential tasks need to be completed in a specific order because they are connected and share the same baseline information.

For example, documenting the Record of Processing Activities (ROPA) provides essential details about data processing, which are then used for drafting Privacy Notices/Policies and performing risk analyses.

Doing these tasks in a logical sequence helps avoid repetitive work and makes the compliance process more efficient.

2

Nonsequential Tasks

Non-sequential tasks are independent of each other and can theoretically be completed in any order.

These tasks, like building and maintaining a Data Protection Management System (DPMS), handling data subject requests, and managing data breaches, don't rely on shared information from other tasks.

Putting Everything Together

No matter where your company is on its compliance journey, this roadmap provides a clear and reusable checklist for every cycle of your Data Protection Management System (DPMS).

Sequential Tasks	Nonsequential Tasks
Record of Processing Activities Identify all processing activities, and document them in a Record of Processing Activities (ROPA) according to Art. 30 GDPR.	**Data Protection Team** Assemble a dedicated team with clear roles and responsibilities. Assess if outside help is required or beneficial. If required, appoint a DPO and notify the Supervisory Authority.
Security Implement and regularly review, update, and improve a security policy ensuring data security through risk-appropriate technical and organizational measures. Document Technical and Organizational Measures (TOM) (Art. 32, 25 GDPR).	**Data Protection Management System** Implement and regularly review, update, and improve a Data Protection Policy to ensure the implementation and maintenance of a Data Protection Management System (DPMS).
Compliance Review Compliance of Processing Activities, including Art. 5 GDPR Principles and the lawfulness of data transfers.	**Data Subject Rights** Implement and regularly review, update, and improve a process for handling data subject requests.
Quick Fixes Any compliance gap that can be closed with low effort or little time should be solved immediately.	**Data Breach** Implement and regularly review, update, and improve a process for handling data breaches and preventing similar incidents in the future.

Sequential Tasks	Nonsequential Tasks
Risk Implement and regularly review, update, and improve a documented process for performing risk assessments and Data Protection Impact Assessments (DPIAs). Perform/Update Risk Analyses and DPIAs (Art. 35 GDPR).	**Data Transfer** Implement and regularly review, update, and improve a process for selecting, changing and terminating data transfers with third parties.
Inform Create new or update existing Privacy Notices for all data subjects and publish them where appropriate.	**Employee Awareness and Training** Implement and regularly review, update, and improve a documented process for employee training and awareness on their contribution and obligation towards data protection and data security.
Deletion Based on the retention and deletion periods documented in the ROPA, create a data retention and deletion plan.	

Navigating Both Checklists

To navigate both checklists, consider the size of your data protection team.

For a single person, prioritize the sequential tasks, as they require more time and effort. Use downtime, such as waiting for feedback, to tackle non-sequential tasks.

If the data protection team includes multiple members, divide the tasks among the team, assigning sequential tasks to those who can focus on building foundational compliance elements, while others handle non-sequential or urgent tasks.

This approach ensures efficient use of resources and steady progress across all areas of GDPR compliance.

8 KEY FEATURES OF AN EFFICIENT DATA PROTECTION STRATEGY

If you are aiming to implement GDPR requirements in the most resource-efficient way, here are some must-have qualities of a strategic plan to implement GDPR requirements:

Strategic Priorization: The plan prioritizes tasks strategically, to maximize efficiency and effectiveness.

Proactive Approach: The plan encourages a proactive rather than reactive approach to anticipate issues before they become urgent.

Comprehensive Coverage: The plan provides comprehensive coverage of GDPR requirements, addressing all aspects of data protection.

Sustainable Processes: The plan develops long-term internal expertise and sustainable processes, ensuring and securing consistency and continuity.

Simple Framework:
The plan offers a clear and logical framework to implement requirements.

Seamless Integration:
The plan integrates seamlessly with existing business processes, minimizing disruption and making compliance more manageable.

Scalability:
The plan adjusts to the company's growth and increasing complexity.

Adaptabilty:
The plan is adaptable to evolving privacy and other related regulations to ensure ongoing compliance.

By including these features, you can ensure your company selects a GDPR compliance plan that is strategic, resource-efficient, and capable of delivering long-term, sustainable compliance.

CONCLUSION

Navigating GDPR compliance is an ongoing challenge that requires a structured and strategic approach.

Many companies, especially those with limited resources, often resort to ineffective compliance implementation methods like ignoring the issue, reactive measures, and random compliance efforts.

Amongst other, these approaches lead to inefficiencies, wasted time, increased risks of fines, data breaches, and higher costs due to duplicated work and urgent fixes.

To address these issues, adopting a strategic approach that prioritizes tasks is crucial.

The Resource-Saving GDPR Roadmap, presented in this whitepaper, distinguishes between sequential and non-sequential tasks.

Sequential tasks require the same baseline information and should be completed in order to leverage synergies and existing documentation, preventing redundant efforts.

Non-sequential tasks are independent and can be prioritized based on immediate needs and resource availability, providing flexibility.

This method streamlines compliance processes and optimizes resource use, ensuring that every action contributes effectively to the overall compliance strategy.

The Resource-Saving GDPR Roadmap guides companies, regardless of their current compliance status, toward efficient and sustainable GDPR compliance.

To learn more about how the Resource-Saving GDPR Roadmap can help your company streamline compliance efforts and optimize resources, request a consultation today at info@melodielange.de.

Shift your compliance approach from a frustrating, slow process to one that is efficient, effective, and yields tangible results.

ABOUT ME

I am Melodie Lange, a data protection and information security consultant since 2017, dedicated to helping companies navigate GDPR compliance efficiently and effectively.

Over the past years, I have assisted numerous clients, from smaller companies to large international enterprises across Europe, in achieving and maintaining GDPR compliance.

My approach to GDPR compliance is pragmatic and efficient, tailored to address the challenges companies face, especially those with limited resources.

I aim to equip companies with the necessary tools to achieve more in months than they previously have in years.

Here are my professional certifications and qualifications in data protection and information security:

- Law Diploma, Ludwig Maximilian University (LMU) in Germany
- Certified Information Privacy Professional/Europe (CIPP/E) by iapp
- Certified Information Privacy Manager (CIPM) by iapp
- Certified Data Protection Officer (IHK)
- Certified Information Security Officer
- ISO IEC 27001 Certified Auditor (TÜV Saarland)
- CompTIA Security+ Certified

Connect with me on LinkedIn or my website for more data protection and privacy compliance insights.

Melodie Lange Privacy & Security Consulting