

# So wird ihr Unternehmen effizient und kostengünstig DSGVO-konform

Für Unternehmensleiter und Compliance-Experten, die es leid sind, Ressourcen zu verschwenden.





# INHALT

Zusammenfassung	4
Der Anhaltende Kampf um die Einhaltung der DSGVO	5
Unwirksame Ansätze zur Einhaltung der DSGVO	7
Der Ressourcensparende DSGVO-Fahrplan	9
Fazit	14
Über Mich	15



## Urheberrecht

Copyright© 2023. Melodie Lange. Alle Rechte vorbehalten. Kein Teil dieses Whitepapers darf durch ein mechanisches, fotografisches oder elektronisches Verfahren oder in Form eines Tonträgers reproduziert werden; es darf auch nicht in einem Datenabfragesystem gespeichert, übertragen oder anderweitig für den öffentlichen oder privaten Gebrauch kopiert werden, mit Ausnahme von „fair use“ als kurze Zitate in Artikeln und Rezensionen, ohne vorherige Genehmigung des Herausgebers.

Diese Publikation soll korrekte und aussagekräftige Informationen zu den behandelten Themen liefern. Sie ist nicht als Rechtsberatung oder als professionelle Dienstleistung gedacht. Wenn Sie fachliche Unterstützung benötigen, wenden Sie sich bitte an einen kompetenten Fachmann.

Design und Umschlaggestaltung von Rizwan Shafique.

Haftungsausschluss: Der Autor übernimmt keine Garantie für die Ergebnisse, die Sie beim Lesen dieses Whitepapers erzielen werden. Die Ergebnisse hängen von der investierten Arbeit und dem Fachwissen der beteiligten Personen ab.

## Zusammenfassung

Die Einhaltung der DSGVO ist kein einmaliges Unterfangen, sondern ein kontinuierlicher Prozess, der ständige Aktualisierungen und Verbesserungen erfordert.

Seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) im Jahr 2018 bleibt der Umgang mit ihr eine Herausforderung für Unternehmen jeder Größe, insbesondere für kleinere Unternehmen mit begrenzten Ressourcen.

Dieses Whitepaper befasst sich mit einem Kernproblem: dem Fehlen einer strukturierten Umsetzungsstrategie, was zu Nichteinhaltung, ineffizienter Ressourcennutzung und Problemen mit den sich weiterentwickelnden Datenschutzbestimmungen führt.

Die vorgestellte Methodik befürwortet einen strategischen Ansatz für die Einhaltung der DSGVO, bei dem die Aufgaben in einer Reihenfolge ausgeführt werden, um die Nutzung der Ressourcen zu optimieren und eine umfassende Einhaltung zu gewährleisten.

Durch die Wiederverwendung bereits erledigter Aufgaben und vorhandener Dokumente können Unternehmen ihre Compliance-Bemühungen optimieren.

Diese Methode bietet eine Alternative für Unternehmen, die nach vergeblichen Bemühungen endlich Ergebnisse erzielen wollen.

Ein strategischer Ansatz verbessert die Einhaltung von Vorschriften, die betriebliche Effizienz, das Engagement der Mitarbeiter und die Kosteneffizienz.

Dieses Whitepaper enthält umsetzbare Empfehlungen und Anleitungen, die zu einer spürbaren Verbesserung der Compliance führen.

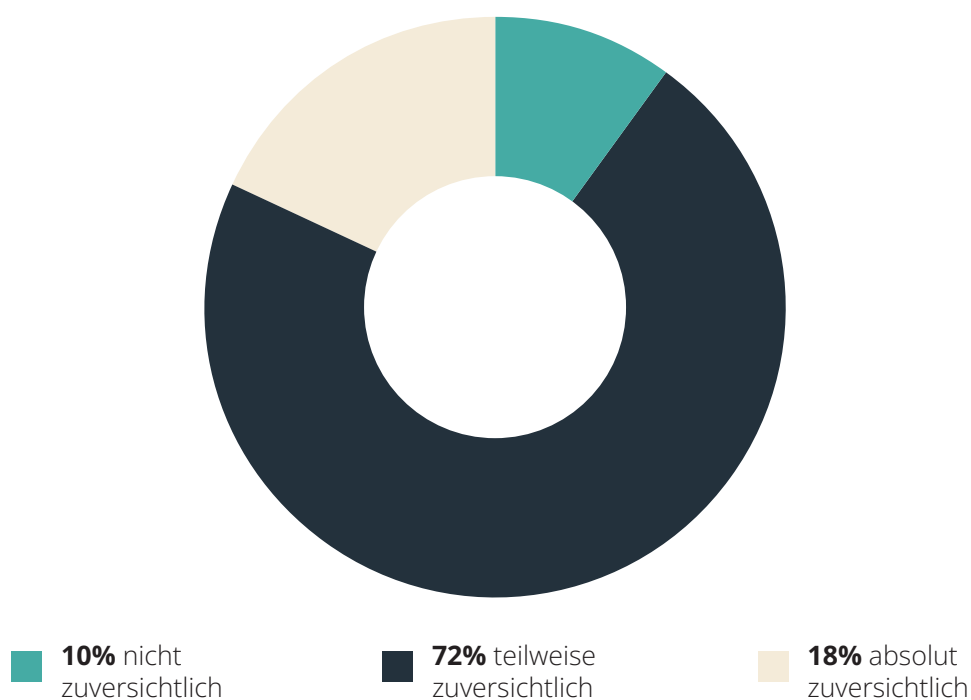
Unabhängig davon, ob es sich um den Beginn oder die Verbesserung eines Compliance-Rahmens handelt, beschleunigt diese Methodik den Fortschritt und sorgt für langfristige Beständigkeit.



# Der anhaltende Kampf um die Einhaltung der DSGVO

Seit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 arbeiten viele Unternehmen immer noch an ihrer anfänglichen To-Do-Liste.

In einem kürzlich veröffentlichten umfassenden Bericht waren nur 2 von 10 befragten Unternehmen vollkommen zuversichtlich, dass ihre Organisation die Datenschutzbestimmungen einhält.



Abgesehen von der Verwirrung über die Anforderungen der DSGVO und deren korrekte Umsetzung wird der Fortschritt bei der Einhaltung der Vorschriften durch den Mangel personeller Ressourcen erheblich behindert. Letzteres ist häufig die Folge begrenzter Budgets.

Es ist verständlich, dass Unternehmen zögern, Geld in Maßnahmen zu investieren, die sich nicht unmittelbar in höheren Gewinnen niederschlagen. Der Bericht zeigt jedoch, dass 41 % der befragten Unternehmen zustimmen und 22 % sogar voll und ganz zustimmen, dass der Mangel an Ressourcen ihre Möglichkeiten zur Erreichung der Ziele einschränkt.

<sup>1</sup> IAPP-EY Privacy Governance Report 2023, S. 9, <https://iapp.org/resources/article/privacy-governance-full-report/>

<sup>2</sup> IAPP-EY Privacy Governance Report 2023, S. 42, <https://iapp.org/resources/article/privacy-governance-full-report/>



**Angesichts begrenzter personeller Ressourcen und Budgets  
müssen alle Maßnahmen zur Einhaltung der DSGVO strategisch  
und effizient sein, um signifikante Ergebnisse zu erzielen.**

Dem Bericht zufolge verfolgen viele Unternehmen jedoch keinen strategischen Ansatz bei der Umsetzung der DSGVO.

Stattdessen „agieren sie eher reaktiv als proaktiv und sind möglicherweise weniger in der Lage, Probleme zu antizipieren ... Datenschutzexperten, die in Unternehmen ohne Datenschutzstrategie arbeiten, müssen sich daher fragen, ob sie ihre Zeit, Ressourcen und Budgets effizient einsetzen.“

Angesichts neuer Datenschutzgesetze sind die Unternehmen noch mehr überfordert und brauchen Hilfe bei der Entscheidung, worauf sie sich konzentrieren sollen.

Dieses Whitepaper dient einem wichtigen Zweck: Es soll Klarheit schaffen und einen strategischen Ansatz bieten, um die Einhaltung der DSGVO auf möglichst ressourceneffiziente Weise zu erreichen und aufrechtzuerhalten.



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

.....

# Unwirksame Ansätze zur Einhaltung der DSGVO

Unternehmen haben verschiedene gängige Ansätze zur Einhaltung der DSGVO gewählt. Diese Methoden erweisen sich jedoch häufig als ineffizient, riskant und kostspielig.

## Gängige Ansätze zur Einhaltung der DSGVO

01

### Das Problem ignorieren.

Ignorieren der Einhaltung der DSGVO in der Hoffnung, dass die Nichteinhaltung keine Konsequenzen haben wird.

02

### Reaktive Compliance

Bearbeitung von DSGVO-Themen nur dann, wenn Audits, Bedenken, Vorgaben der Unternehmensleitung oder externe Notfälle wie Datenschutzverletzungen, Betroffenenanfragen oder Medienaufmerksamkeit sofortiges Handeln erfordern.

03

### Willkürliche Compliance

Sporadische Umsetzung von Maßnahmen zur Einhaltung der DSGVO ohne kohärenten Plan oder wenn es dringend wird.

## Die Nachteile

Eine unstrategische Umsetzung der DSGVO führt zu Ineffizienzen und erhöhten Risiken und verursacht erhebliche finanzielle Kosten. Diese Herausforderungen zeigen sich in drei kritischen Bereichen.



### Zeit

Das Ignorieren der Einhaltung der DSGVO oder die Umsetzung sporadischer Maßnahmen ohne kohärenten Plan führen zu Ineffizienz, verzögern den Fortschritt und verlängern den Zeitraum der Nichteinhaltung.

Darüber hinaus wird der Geschäftsbetrieb gestört, die Aufmerksamkeit von den Kerntätigkeiten abgelenkt und Gesamtproduktivität verringert, wenn in Krisensituationen, Korrekturen in letzter Minute vorgenommen werden müssen.



### Risiko

Unternehmen, welche die DSGVO nicht konsequent einhalten, setzen sich erheblichen Risiken aus und erhöhen die Wahrscheinlichkeit von Bußgeldern, Datenschutzverletzungen und rechtlichen Maßnahmen.

Die Nichteinhaltung kann den Ruf eines Unternehmens schädigen, das Vertrauen und die Loyalität von Kunden gefährden und zu Geschäftseinbußen und Wettbewerbsnachteilen führen.



### Geld

Unzureichende DSGVO-Compliance-Praktiken können erhebliche finanzielle Folgen in Form von Bußgeldern, rechtlichen Schritten und Rufschädigung nach sich ziehen.

Darüber hinaus werden die hohen Kosten reaktiver Compliance-Maßnahmen häufig übersehen, da dringende Korrekturen in letzter Minute mehr Ressourcen erfordern als eine proaktive Planung

## Schlussfolgerungen

Um diese Gefahren zu vermeiden, müssen Unternehmen einen strategischen und proaktiven Ansatz zur Einhaltung der DSGVO verfolgen und sicherstellen, dass ihre Bemühungen effizient, gut koordiniert und kosteneffektiv sind.



.....

# Der Ressourcensparende DSGVO-Fahrplan

## DSGVO-Aufgaben Identifizieren

Um die Einhaltung der DSGVO langfristig und ressourceneffizient zu erreichen und aufrechtzuerhalten, müssen die folgenden zwei Aufgabenkategorien umgesetzt werden: sequentielle Aufgaben und nicht sequentielle Aufgaben.

Diese Unterscheidung hilft, den Compliance-Prozess effektiver zu organisieren und zu priorisieren.

### 1 Sequenzielle Aufgaben

Sequenzielle Aufgaben müssen in einer bestimmten Reihenfolge durchgeführt werden, da sie zusammenhängen und dieselben grundlegenden Informationen enthalten.

Beispielsweise liefert das Verzeichnis der Verarbeitungstätigkeiten (VVT) wichtige Details über die Datenverarbeitung, die für die Erstellung von Datenschutzhinweisen und Durchführung von Risikoanalysen verwendet werden können.

Die logische Abfolge dieser Aufgaben hilft, redundante Arbeiten zu vermeiden und den Compliance-Prozess effizienter zu gestalten.

### 2 Nicht Sequenzielle Aufgaben

Nicht sequentielle Aufgaben sind voneinander unabhängig und können theoretisch in beliebiger Reihenfolge ausgeführt werden.

Diese Aufgaben, wie z. B. die Einrichtung und Pflege eines Datenschutzmanagementsystems (DSMS), die Bearbeitung von Betroffenenanfragen und Datenschutzverletzungen, beruhen nicht auf gemeinsame Informationen

## Zur Umsetzung

Unabhängig davon, wo sich Ihr Unternehmen auf dem Weg zur Einhaltung der Datenschutzvorschriften befindet, dieser Fahrplan bietet eine klare und wiederverwendbare Checkliste für jeden Zyklus Ihres Datenschutzmanagementsystems (DSMS).

Sequenzielle Aufgaben	Nonsequential Tasks
<p><b>Verzeichnis der Verarbeitungstätigkeiten</b></p> <p>Identifizieren Sie alle Verarbeitungstätigkeiten und dokumentieren Sie diese in einem Verzeichnis der Verarbeitungstätigkeiten (VVT) gemäß Art. 30 DSGVO.</p>	<p><b>Datenschutz-Team</b></p> <p>Stellen Sie ein Team mit klaren Rollen und Verantwortlichkeiten zusammen. Prüfen Sie, ob externe Unterstützung notwendig oder sinnvoll ist. Ernennen Sie ggf. einen Datenschutzbeauftragten und benachrichtigen Sie die Aufsichtsbehörde.</p>
<p><b>Sicherheit</b></p> <p>Umsetzung und regelmäßige Überprüfung, Aktualisierung und Verbesserung einer Sicherheitspolitik, die die Datensicherheit durch risikogerechte technische und organisatorische Maßnahmen gewährleistet.</p> <p>Dokumentation der technischen und organisatorischen Maßnahmen (Art. 32, 25 DSGVO).</p>	<p><b>Datenschutzmanagementsystem</b></p> <p>Umsetzung und regelmäßige Überprüfung, Aktualisierung und Verbesserung einer Datenschutzpolitik, um die Einführung und Aufrechterhaltung eines Datenschutzmanagementsystems (DPMS) zu gewährleisten.</p>
<p><b>Compliance</b></p> <p>Überprüfung der Konformität der Verarbeitungstätigkeiten, gemäß Art. 5 DSGVO sowie der Rechtmäßigkeit der Datenübermittlungen.</p>	<p><b>Betroffenenrechte</b></p> <p>Einführung und regelmäßige Überprüfung, Aktualisierung und Verbesserung eines Prozesses zur Bearbeitung von Anfragen betroffener Personen.</p>
<p><b>Schnelle Lösungen</b></p> <p>Jede Konformitätslücke, die mit geringem Aufwand oder in kurzer Zeit geschlossen werden kann, sollte sofort geschlossen werden.</p>	<p><b>Datenschutzvorfall</b></p> <p>Einführung und regelmäßige Überprüfung, Aktualisierung und Verbesserung eines Prozesses zum Umgang mit Datenschutzvorfällen und zur Vermeidung ähnlicher Vorfälle in der Zukunft.</p>

Sequenzielle Aufgaben	Nonsequential Tasks
<p><b>Risiko</b></p> <p>Einführung und regelmäßige Überprüfung, Aktualisierung und Verbesserung eines dokumentierten Prozesses zur Durchführung von Risikobewertungen und Datenschutz-Folgenabschätzungen (DSFAs).</p> <p>Durchführung/Aktualisierung von Risikoanalysen und DSFAs (Art. 35 DSGVO).</p>	<p><b>Datentransfer</b></p> <p>Einführung und regelmäßige Überprüfung, Aktualisierung und Verbesserung eines Prozesses zur Auswahl, Änderung und Beendigung von Datenübermittlungen an Dritte.</p>
<p><b>Informieren</b></p> <p>Erstellen neuer oder aktualisieren bestehender Datenschutzhinweise für alle betroffenen Personen.</p>	<p><b>Sensibilisierung und Schulung</b></p> <p>Einführung und regelmäßige Überprüfung, Aktualisierung und Verbesserung eines dokumentierten Prozesses zur Schulung und Sensibilisierung der Mitarbeiter für ihren Beitrag und ihre Verpflichtung zum Datenschutz und zur Datensicherheit.</p>
<p><b>Löschung</b></p> <p>Erstellen eines Prozesses zur Aufbewahrung und Löschung von Daten auf der Grundlage der im VT dokumentierten Aufbewahrungs- und Löschungsfristen.</p>	

## Navigieren beider Checklisten

Berücksichtigen Sie bei der Bearbeitung der beiden Checklisten die Größe Ihres Datenschutzteams.

Wenn Sie nur eine Person haben, sollten Sie den sequentiellen Aufgaben den Vorrang geben, da sie mehr Zeit und Aufwand erfordern. Nutzen Sie Leerlaufzeiten, wie z. B. das Warten auf Feedback, um nicht sequentielle Aufgaben zu erledigen.

Besteht das Datenschutzteam aus mehreren Mitgliedern, teilen Sie die Aufgaben derart auf, indem Sie die sequentiellen Aufgaben denjenigen zuweisen, die sich auf die Entwicklung grundlegender Compliance-Elemente konzentrieren können, während die anderen die nicht sequentiellen oder dringenden Aufgaben erledigen.

Dieser Ansatz gewährleistet eine effiziente Nutzung der Ressourcen und stetige Fortschritte in allen Bereichen der DSGVO-Compliance.

## 8 Wesentliche Merkmale einer Effizienten Datenschutzstrategie

Wenn Sie die Anforderungen der DSGVO so ressourceneffizient wie möglich umsetzen möchten, finden Sie hier einige Merkmale, die ein strategischer Plan zur Umsetzung der DSGVO unbedingt aufweisen sollte:



### **Strategische Priorisierung:**

Der Plan setzt strategische Prioritäten, um Effizienz und Effektivität zu maximieren.



### **Proaktiver Ansatz:**

Der Plan fördert einen proaktiven statt eines reaktiven Ansatzes, um Probleme zu antizipieren, bevor sie kritisch werden.



### **Umfassende Absicherung:**

Der Plan deckt die Anforderungen der DSGVO umfassend ab und behandelt alle Aspekte des Datenschutzes.



### **Nachhaltige Prozesse:**

Der Plan entwickelt langfristiges internes Fachwissen und nachhaltige Prozesse, die Beständigkeit und Kontinuität gewährleisten und sicherstellen.



### **Einfaches Framework:**

Der Plan bietet einen klaren und logischen Ansatz für die Umsetzung der Anforderungen.



### **Nahtlose Integration:**

Der Plan fügt sich nahtlos in bestehende Geschäftsprozesse ein, was Störungen minimiert und die Einhaltung der Anforderungen erleichtert.



### **Skalierbarkeit:**

Der Plan passt sich dem Wachstum des Unternehmens und der zunehmenden Komplexität an.



### **Anpassungsfähigkeit:**

Der Plan kann an sich ändernde Datenschutz- und andere Vorschriften angepasst werden, um eine kontinuierliche Einhaltung zu gewährleisten.

Durch die Einbeziehung dieser Merkmale können Sie sicherstellen, dass Ihr Unternehmen einen Plan zur Einhaltung der DSGVO auswählt, der strategisch und ressourceneffizient ist und eine langfristige, nachhaltige Einhaltung der Vorschriften gewährleistet.



## Fazit

Die Einhaltung der DSGVO ist eine ständige Herausforderung, die einen strukturierten und strategischen Ansatz erfordert.

Viele Unternehmen, insbesondere solche mit begrenzten Ressourcen, greifen häufig auf ineffiziente Methoden zurück, um die Einhaltung zu gewährleisten, wie z. B. Ignorieren des Problems, reaktive Maßnahmen und willkürliche Bemühungen um die Einhaltung.

Diese Ansätze führen unter anderem zu Ineffizienz, Zeitverschwendung, einem erhöhten Risiko von Bußgeldern, Datenschutzverletzungen und höheren Kosten aufgrund von Doppelarbeit und dringenden Abhilfemaßnahmen.

Um diese Probleme zu lösen, ist ein strategischer Ansatz, der Aufgaben strategisch priorisiert, von entscheidender Bedeutung.

Der in diesem Whitepaper vorgestellte Ressourcensparende DSGVO-Fahrplan unterscheidet zwischen sequentiellen und nicht-sequentiellen Aufgaben.

Sequentielle Aufgaben erfordern die gleichen grundlegenden Informationen und sollten in einer logischen Reihenfolge abgeschlossen werden, um Synergien und vorhandene

Dokumentation zu nutzen und redundante Arbeit zu vermeiden. Nicht-sequentielle Aufgaben sind unabhängig und können je nach unmittelbarem Bedarf und Verfügbarkeit von Ressourcen priorisiert werden, was Flexibilität bietet.

Dieser Ansatz strafft die Compliance-Prozesse und optimiert die Ressourcennutzung, wodurch sichergestellt wird, dass jede Maßnahme einen wirksamen Beitrag zur gesamten Compliance-Strategie leistet.

Der Ressourcensparende DSGVO-Fahrplan führt Unternehmen unabhängig von ihrem aktuellen Compliance-Status zu einer effizienten und nachhaltigen DSGVO-Compliance.

Wenn Sie mehr darüber erfahren möchten, wie der Ressourcensparende DSGVO-Fahrplan Ihrem Unternehmen helfen kann, Compliance-Bemühungen zu rationalisieren und Ressourcen zu optimieren, fordern Sie noch heute ein Beratungsgespräch an: [info@melodielange.de](mailto:info@melodielange.de).

Verwandeln Sie Ihren Compliance-Ansatz von einem frustrierenden und langsamen Vorgang in einen effizienten und effektiven Prozess, der greifbare Ergebnisse liefert.

.....

## Über Mich

Mein Name ist Melodie Lange und seit 2017 unterstütze ich als Beraterin für Datenschutz und Informationssicherheit Unternehmen bei der effizienten und effektiven Umsetzung der DSGVO.

In den vergangenen Jahren habe ich zahlreiche Kunden, von kleinen Unternehmen bis hin zu großen internationalen Konzernen in ganz Europa, bei der Einhaltung der DSGVO unterstützt.

Mein Ansatz zur Einhaltung der DSGVO ist pragmatisch und effizient und auf die Herausforderungen zugeschnitten, denen sich Unternehmen, insbesondere solche mit begrenzten Ressourcen, gegenübersehen.

Mein Ziel ist es, Unternehmen in die Lage zu versetzen, in wenigen Monaten mehr zu erreichen als in vielen Jahren zuvor.

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

- Zertifizierte Datenschutzbeauftragte (IHK)
- Certified Information Privacy Professional / Europe (CIPP/E)
- Certified Information Privacy Manager (CIPM)
- Zertifizierte ISO IEC 27001 Auditorin (TÜV)
- CompTIA Security+ zertifiziert
- IT-Sicherheitsbeauftragter nach ISO/IEC 27001/27002 und BSI IT-Grundschutz

Besuchen Sie mich auf [LinkedIn](#) oder auf meiner Website. Dort finden Sie weitere Informationen zum Datenschutz und zur Einhaltung der Datenschutzbestimmungen.



