## Ihr Gesamt-Bewertungsresultat zur EU-DSGV-Vorbereitung

IDC definiert fünf Reifestadien der Vorbereitung auf die EU-DSGV: Wer gerade beginnt, befindet sich in Stadium 1, Unternehmen, die volle Konformität erreicht haben, befinden sich in Stadium 5. Basierend auf Ihren Antworten befindet sich Ihre Organisation im **Stadium 2 - Beschleunigung**.

Zusätzlich haben wir evaluiert, in welchem der fünf Stadien Sie sich auf jedem der folgenden drei Gebiete der EU-DSGV befinden. So gewinnen Sie einen guten Eindruck davon, worauf Sie sich besonders konzentrieren müssen. Diese Themen sind:

- Allgemeine Herangehensweise an die EU-DSGV
- Zielsetzung, Bewusstsein über die vorhandenen Daten
- Risikobewusstsein, Eisikoeinschätzung, Risikominimierung

## Allgemeine Herangehensweise an die EU-DSGV, Zielsetzung und Führungsstruktur

Bei der EU-DSGV geht es nicht nur um IT-Sicherheit. Sie berührt das Datenschutz-Konzept und die Datenschutzkultur eines Unternehmens. Um erfolgreich zu sein, müssen Sie für die unverzichtbare Unterstützung des gesamten Unternehmens werben - vom Top-Management bis zu den einzelnen Geschäftsbereichen. Um die Regeln nachhaltig und langfristig einzuhalten, gilt es, eine Kultur gemeinsamer Verantwortung zu entwickeln.

# Stadium 1: Initiierung

Sie haben viel zu tun. Organisationen in dieser Kategorie, die erst die ersten Schritte einer Vorbereitung bewältigt haben, haben nur begrenztes oder kein Wissenüber die Auforderungen und (noch wichtiger) die Auswirkungen der EU-DSGV auf ihr Geschäft. Das Führungspersonal hat keinerlei echtes Verständis davon, was die EU-DSGV abdeckt und wie sie implementiert wird. Zusätzlich fehlt auch ein echtes Verständnis von rechtlichen Verpflichtungen und Verantwortung oder des Umfang der Geldbußen und anderer Saktionen, wenn das Unternehmen nicht bis zum Mai kommenden Jahres regelkonform wird.

Wie Sie selbst angegeben haben, beginnen Sie gerade erst mit der Umsetzung der EU-DSGV. Sie betrifft nahezu alle Unternehmen, die personenbezogene Daten verarbeiten. Seien Sie sich darüber im Klaren, dass die Definition personenbezogener Daten sehr weit gefasst ist und alle Daten einschließt, die sich auf eine identifizierbare Person beziehen. Auf der einfachsten Ebene sind das Mitarbeiterdaten und Daten, die sich auf Bestellungen beziehen. Die meisten Organisationen besitzen solche Daten. Deshalb ist es sehr wahrscheinlich, dass auch Sie von der EU-DSGV betroffen sind.

Die GDPR zu ignorieren, ändert daran nichts. Es ist wichtig zu wissen, dass substantielle Sanktionen angedroht werden, um zur Regelkonformität zu zwingen. Viel wurde schon über die erheblichen Geldbußen gesprochen. Darüber hinaus gehören zu den Saktionen auch Gemeinschaftsklagen und die Aussetzung der Verarbeitung personenbezogener Daten (was im Endeffekt auf ein Verbot von Handelsaktivitäten hinausläuft).

Der Status Ihrer Vorbereitungen wurde besser bewertet, weil Sie damit begonnen haben, eine funktionsübergreifende Compliance-Task-Force oder ein Steuerungsgremium in Ihrer Organisation aufzubauen. Das Engagement aller relevanten Interessenträger ist ein kritischer Erfolgsfaktor für jedes Programm zur Umsetzung der EU-DSGV. Die Existenz einer solchen koordinierten Herangehemsweise steigert letztlich den Erfolg aller Compliance-Aktivitäten. Ein weiterer kritischer Faktor ist, wer das EU-DSGV-Programm leitet. Es ist weniger wichtig, wohner das Führungspersonal stammt, als dass es Autorität, Wissen und Charisma genug hat, strategisch wichtige Programme oder Aktivitäten anzuführen.

## Datenbewusstsein (Data Awareness)

Information Governance (die Steuerung und das Management aller im Unternehmen vorhandenen Informationen) ist für die Einhaltung der Regeln der EU-DSGV unabdingbar. Sämtliche personenbezogenen Daten müssen in den Zuständigkeitsbereich der Inforation-Governance-Funktion fallen. Sie müssen wissen, welche personenbezogenen Daten Sie haben (entsprechend der in der EU-DSGV verwendeten, sehr breiten Definition) und auch ihren Standort, Zustimmungen, Lebensdauer und so weiter kennen. Dem Regulator nachzuweisen, dass Sie Ihre Daten gut handhaben, ist der erste Schritt zur Compliance.

# Stadium 1: Initiierung

Leider befinden Sie sich noch in einem sehr frühen Stadium der Information Governance. Sie haben nur geringes Vertrauen in Ihre Fähigkeit, Daten zu identifizieren und zu lokalisieren. Sie mögen zwar Ihre strukturierten Daten gut verstehen, aber Ihre unstrukturierten Daten könnten Probleme verursachen. Wahrscheinlich sammeln Sie auch Daten, ohne genau zu wissen wozu oder was ihr geschäftlicher Wert ist. Durch die EU-DSGV werden sie zu risikobehafteten Daten, also müssen Sie entscheiden, ob Sie sie tatsächlich behalten oder lieber löschen wollen.

Nach Ihrem Stadium zu schließen, werden Sie wahrscheinlich Schwierigkeiten haben, Datenzugriffsanfragen von Datensubjekten und anderen neuen Rechten zu entsprechen, die die EU-DSGV definiert (einschließlich des "Rechts auf Vergessenwerden").

Sie gehören zu der kleinen Minderheit von Organisationen, die volles Vertrauen in ihre Fähigkeit besitzen, alle Instanzen personenbezogener Daten in ihrer Organisation identifizieren und lokalisieren zu können. Gut gemacht. Aber stellen Sie sicher, dass Ihre Mitarbeiter keine eigenen Datenkopien erzeugen - wahrscheinlich tun sie das aus guten Gründen -, die dann nicht mehr den Regeln entsprechen. Es werden oft Daten kopiert: für Berichte, Analysen, Datensicherung und so weiter. Stellen Sie sicher, einen Prozess zu implementieren, der das zukünftig verhindert.

Kurz gesagt, Sie haben kein Datenbewusstsein. Das Wissen darüber, welche Daten in der Organisation vorhanden sind, wo sie liegen und warum sie gespeichert werden ist eine Grundvoraussetzung für Konformität zur EU-DSGV. Das ist notwendig, um ein Datenverarbeitungsverzeichnis zu erstellen, wie es Artikel 30 EU-DSGV vorschreibt. Wahrscheinlich handeln Sie auch gegen die Prinzipien der Zweckbindung, Datenminimierung und Speicherbegrenzung. Sie müssen entscheiden, ob Sie mit diesen Risiken leben können.

Wo anfangen? Unter dem gegebenen Zeitdruck müssen Sie die für Sie wertvollsten oder die risikobehaftetsten Daten priorisieren. Alle sensitiven Daten (spezielle Kategorien) sind davon betroffen, genauso Daten, die, wenn sie von einem Datenschutzzwischenfall betroffen wären, Ihren Ruf schädigen könnten. Natürlich ist es nur einer von vielen Schritten, diese Daten zu schützen. Sie müssen sich auch dringend mit den Prozessen befassen, die mit den Daten interagieren. Es ist rechtlich verpflichtend klar zu definieren, wer Zugriff auf welche Daten hat

und zu welchem Zweck.

Vor allem sollten Sie davon ausgehen, dass der Regulierer voraussichtlich Datenschutzzwischenfälle und kleinere Inkonformitäten tolerieren wird. Keine Toleranz wird es für fehlende oder nicht belegte Anstrengungen, Konformität zu erreichen, geben. Es reicht nicht, zu wissen welche Daten man hält und wo sie liegen: Sie müssen das auch belegen können.

## Risikobewusstsein, -bewertung und -begrenzung

In der EU-DSGV geht es vor allem um Risiken. Ihre meisten Anforderungen sind hinsichtlich der Umsetzungsweise nicht bindend - Organisationen müssen also selbst entscheiden, welche Herangehensweise sie wählen. Wie schwer wiegen das Bedürfnis, Daten für Analysen zu sammeln gegenüber dem erhöhten Risiko hinsichtlich der Prinzipien Datensparsamkeit und Zweckbindung? Was zum Teufel ist der "Stand der Technik" (State of the Art) und woher weiß man, ob es notwendig ist, ihn zu implementieren?

Risikobewusstsein beginnt mit Selbstanalyse: Welche Daten sind vorhanden und wie beeinflussen die neuen Regeln ihre Handhabung?

# Stadium 1: Initiierung

Anscheinend befinden Sie sich in einem frühen Stadium des Risikobewusstseins. Sie scheinen sich zu bemühen, die richtigen Fragen zu stellen, aber nur auf einer grundlegenden Ebene. Einige Basisanforderungen stellen Sie vor Herausforderungen. Sie scheinen die EU-DSGV weniger ernst zu nehmen als man meinen sollte, wenn Sie die neuen Regeln tiefgehend verstanden hätten. Ihr Kampf um Budget und Ressourcen reflektiert ihre noch niedrige Bewusstseinsebene, speziell auf Vorstandsebene.

Ihre Antwort zeigt, dass Sie hinsichtlich Cloud-Nutzung und Datenschutz einen hohen Reifegrad erreicht haben. Dazu kann die Anpassung bestehener Cloud-Services gehören, um sicherzustellen, dass sie konform zu den neuen Regeln sind. Oder dass Sie bereits sichergestellt haben, dass Ihre Form der Cloud-Nutzung rechtskonform ist und nicht weiter verändert werden muss. Wenn das stimmt, dann ist das großartig: Sie sind den meisten weit voraus. Aber seien Sie gewarnt: Die Konsequenzen einer falschen Cloud-Nutzung, beispielsweise durch die Annahme, dass der Cloud-Provider die volle rechtliche Verantwortung übernehmen kann (das kann er nicht), können schwerwiegend sein. Sorgen Sie dafür, dass Ihre Cloud-Verträge durchgesehen und gründlich auf EU-DSGV-Konformität geprüft werden.

Sie scheinen eine ausgewogene Perspektive hinsichtlich der mit der EU-DSGV verbundenen Risiken zu haben. Das bedeutet, dass Sie die potentiellen Auswirkungen fehlender Konformität vollständig verstanden haben, nicht nur bezüglich möglicher Geldbußen, sondern auch hinsichtlich von Rufschädigungen, Gemeinschaftsklagen und der Einstellung von Datenverarbeitungsaktivitäten. Trotzdem befinden Sie sich noch in einem frühen Stadium der EU-DSGV-Konformität - machen Sie weiter!