„Bei Verstößen drohen Bußgelder in Höhe von bis zu 4 % des weltweiten Unternehmensumsatzes“
(Art. 83 Abs. 5 DSGVO)

mVISE informiert: EU-DSGVO tritt am 25. Mai 2018 in Kraft

Am 25. Mai 2018 endet die zweijährige Übergangsfrist für die neue europäische Datenschutzgrundverordnung (DSGVO/GDPR). Unternehmen müssen ab diesem Zeitpunkt die neue Richtlinie berücksichtigen und deren Anforderungen ausreichend und nachweisbar umsetzen. Mit der am 14. April 2016 beschlossenen Vereinheitlichung des europäischen Datenschutzrechts drohen bei Datenschutzverstößen Bußgelder in Höhe von bis zu 4% des weltweiten Unternehmensumsatzes.

DSGVO auf einem Blick

Am 14. April 2016 wurde die DSGVO durch das EU-Parlament beschlossen. Nach Veröffentlichung im Amtsblatt der Europäischen Union, trat diese am 24. Mai 2016 in Kraft. Bis zu diesem Zeitpunkt haben Unternehmen, die persönliche Daten von EU-Bürgern verarbeiten oder speichern, Zeit, den Anforderungen der neuen Richtlinien zu entsprechen. Das oberste Ziel der Verordnung ist dabei der Schutz der Grundrechte und -freiheiten natürlicher Personen und deren Recht auf den Schutz personenbezogener Daten sowie deren freien Verkehr. Die Ziele der DSGVO sollen durch die in Art. 5 DSGVO festgelegten Grundsätze der Verarbeitung personenbezogener Daten erreicht werden.

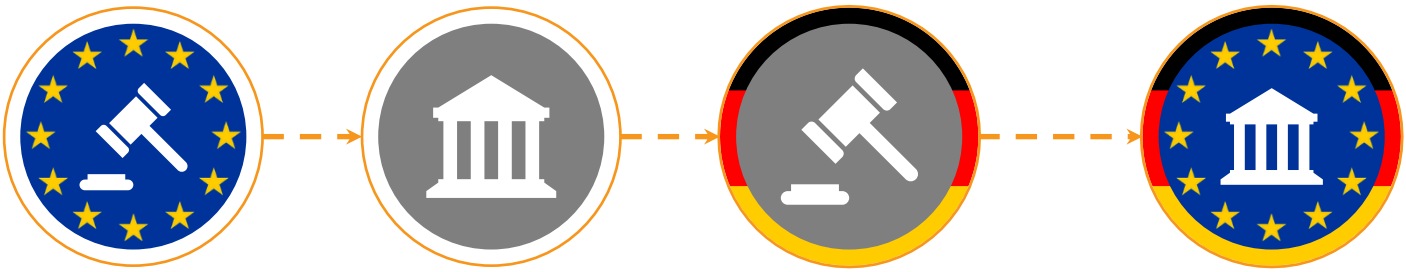
Art. 5 DSGVO regelt die

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Anwendungsbereich DSGVO

Bei der Anwendung der DSGVO wird zwischen einem sachlichen und einem räumlichen Anwendungsbereich unterschieden (Art. 2, 3 DSGVO).

Der **sachliche Anwendungsbereich** definiert, ob die DSGVO in einem Unternehmen Anwendung findet. Art. 2 DSGVO besagt, dass die Verordnung für die Verarbeitung personenbezogener Daten, welche in einem Dateisystem gespeichert sind oder werden sollen, gilt. Keine Anwendung findet die Verordnung, falls keine personenbezogenen Daten verarbeitet werden oder bei Daten, die keiner festgelegten Ordnung unterliegen (bspw. lose Papierakten).



14. April 2016
DSGVO
beschlossen

24. Mai 2016
DSGVO
in Kraft getreten

12. Mai 2017
BDSG (neu)
beschlossen

25. Mai 2018
DSGVO Ende der
Übergangsfrist
BDSG (neu) tritt in Kraft

mVISE AG | Wanheimer Straße 66 | 40472 Düsseldorf | security@mvise.de | +49 211 781 780 0 | www.mvise.de

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Der **räumliche Anwendungsbereich** definiert, wo die DSGVO Anwendung findet. Für Unternehmen mit einer Niederlassung in der EU trifft diese zu. Dabei spielt es keine Rolle, ob es sich um die Filiale eines Verantwortlichen oder eines Auftragsverarbeiters handelt. Wichtig ist, dass sämtliche Unternehmen und deren Niederlassungen von der DSGVO betroffen sind, sobald personenbezogene Daten von EU-Bürgern gespeichert oder verarbeitet werden, unabhängig davon, ob dieser Prozess innerhalb oder außerhalb der EU durchgeführt wird.

Auftragsdatenverarbeitung bezeichnet die Erhebung, Verarbeitung oder Speicherung personenbezogener Daten im Auftrag einer anderen Stelle.

Eine weitere Regelung gilt für Niederlassungen außerhalb der EU. Hier greift das sog. „Marktortprinzip". Dies bedeutet, dass die DSGVO greift, sobald das jeweilige Leistungsangebot für den europäischen Markt bestimmt ist (bspw. chinesische Anbieter, die ihre Waren in der EU anbieten). Damit soll bezweckt werden, dass bei Geschäften in der EU die Voraussetzungen der DSGVO eingehalten werden müssen, wodurch hohe Datenschutzbestimmungen und Wettbewerbsbedingungen geschaffen werden können.

Betroffen sind u.a. alle Exporteure, Versandhändler, Betreiber von Portalen für Onlinebestellungen und jegliche Dienstleister, vorausgesetzt die Leistungen werden in der EU angebo-

Strafen bei Datenschutzverstößen

Bislang waren Bußgelder in Millionenhöhe bei Datenschutzverstößen in der EU eine Seltenheit. Dies kann sich allerdings mit Inkrafttreten der neuen DSGVO ändern. Art. 83 Abs. 4-6 DSGVO gibt Auskunft über die Höhe der Bußgelder. Bei Nichteinhaltung der DSGVO kann nach Art. 83 Abs. 5 DSGVO die Höchststrafe für Unternehmen bis zu 20 Mio. Euro oder 4 Prozent des weltweiten jährlichen Umsatzes betragen. Einen abgestuften Ansatz zu den Bußgeldern macht Art. 83 Abs. 4 DSGVO. Demnach kann einem Unternehmen bei Nichteinhaltung der DSGVO ein Bußgeld von bis zu 10 Mio. Euro oder 2 Prozent des weltweiten jährlichen Umsatzes des vorangegangenen Geschäftsjahrs verhängt werden.

Benennung des Datenschutzbeauftragten nach DSGVO

Nach der neuen DSGVO ist die Benennung eines Datenschutzbeauftragten (DSB) ab dem 25. Mai 2018 verpflichtend, sobald die Tätigkeit des Unternehmens aus datenschutzrechtlicher Sicht einer besonderen Kontrolle bedarf. Eine Ausnahme besteht bei der Verarbeitung personenbezogener Daten durch ein Gericht, da diese im Rahmen ihrer justiziellen Tätigkeit handeln. Des Weiteren ist ein DSB verpflichtend, sobald das Kerngeschäft des Unternehmens in der Überwachung und dem Umgang mit personenbezogenen Daten liegt oder besondere personenbezogene Daten nach Art. 9 und 10 DSGVO verarbeitet werden.

Neu ist, dass die Bestellung eines DSB nach DSGVO nicht mehr an eine Mindestanzahl an Beschäftigten geknüpft ist. Für manche Mitgliedsstaaten bedeutet dies, dass die Zahl der zur Bestellung eines DSB verpflichteten Unternehmen drastisch reduzieren wird, es sei denn, sie machen Gebrauch von der

Öffnungsklausel in Art. 37 Abs. 4 DSGVO. Diese hat zur Folge, dass einzelne Mitgliedsstaaten von der europaweiten Richtlinie abweichen können, falls die Benennung eines DSB nach Recht des Mitgliedsstaates vorgeschrieben ist. In Deutschland wird die „ursprüngliche“ Regelung des BDSG aufrecht gehalten, wodurch es in Deutschland zu keinen drastischen Veränderungen bei der Benennung eines DSB kommen wird. In alle anderen Mitgliedsstaaten, bei denen die DSGVO greift, haben Organisationen aber dennoch das Recht, freiwillig einen DSB zu benennen. Des Weiteren wird der Prozess für die Bestellung des DSB wird vereinfacht. Für diesen Vorgang reicht es aus, den DSB zu „benennen“. Eine schriftliche Bestellung wird nicht mehr gefordert. Dennoch müssen nach Art. 37 Abs. 7 DSGVO die Kontaktdaten des DSB veröffentlicht und der Aufsichtsbehörde mitgeteilt werden. Ebenfalls ist es nach Art. 37 Abs. 2 DSGVO möglich, einen DSB für mehrere Standorte zu benennen. Diese Regelung gilt allerding nur für Unternehmensgruppen, deren Niederlassungen für den DSB leicht zu erreichen sind.

Vorteile eines externen DSB:

- Konzentration auf das Kerngeschäft
- Nachweisbare Fachkunde
- Risikominimierung in der Haftung
- Transparente Kostenstruktur
- Keine Bindung von Ressourcen
- Unvoreingenommene Herangehensweise
- Kündigung jederzeit möglich
- Stellvertretung jederzeit gesichert
- Keine Interessenskonflikte
- Neutrale Position

Weiterhin besteht die Möglichkeit, die Position des DSB intern oder extern zu besetzen. Da die Benennung eines externen Datenschutzbeauftragten einige Vorteile mit sich bringt, machen Unternehmen von dieser Möglichkeit oft gebrauch. Art. 37 Abs. 6 DSGVO regelt die Möglichkeit der Besetzung der Position als betrieblichen DSB.

DSGVO im PDCA-Zyklus

Die DSGVO lässt sich wie ein Informationssicherheits-Managementsystem (ISMS) in einem PDCA-Zyklus abbilden. Dieser ist einfach anzuwenden, lässt sich in allen Organisationsbereichen nutzen und muss lediglich in der Anwendung auf die spezifische Aufgabenstellung hin angepasst werden. Zu Beginn des PDCA-Zyklus bedarf es einer Initialisierungsphase, um das Projekt zu organisieren und zu starten sowie die nachfolgenden vier Phasen: **P**lan, **D**o, **C**heck, **A**ct. Die Inhalte jeder einzelnen Phase werden nachfolgend erläutert.

Für eine erfolgreiche Durchführung und Initialisierung eines DSGVO-Projektes bedarf es einiger vorbereitender Schritte. Wichtig ist, das Projekt zur DSGVO nicht als einmaliges Projekt anzusehen. Viel mehr bedarf es einer ständigen Verbesserung und Anpassung im Rahmen eines kontinuierlichen Verbesserungsprozesses (KVP) für das zu entwickelnde Managementsystem. Im Vorfeld ist es hilfreich, bestehende Leitfäden und Hilfen sowie Datenschutz-Compliance und -Prozesse zu evaluieren, um daraus mögliche Aspekte für das eigene DSGVO Projekt abzuleiten. Für eine schnelle und reibungslose Durchführung des Projekts ist es ratsam, Hilfe von Fachexperten im Bereich Datenschutz- und Managementsysteme in Anspruch zu nehmen. Neben der Evaluation ist es von großer Wichtigkeit, eine geeignete Projektstruktur auszuwählen. Alle Adressaten des DSGVO Projekts müssen bekannt sein. Gleichzeitig wird eine geeignete Dokumentationsstruktur benötigt.

Ob hierbei aufgrund von Kosten auf eine Office-Lösung oder ein spezielles, für ein Datenschutzmanagementsystem geeignetes Tool, zurückgegriffen wird, ist der jeweiligen Organisation überlassen. Zur Reduzierung des Arbeits- und Pflegeaufwands wird allerdings die Verwendung eines Tools empfohlen. Ein weiterer wichtiger Schritt in der Initialisierungsphase ist das Festlegen geeigneter Informations- und Kommunikationswege. Hierdurch kann im weiteren Verlauf ein fehlerfreier Informationsaustausch gewährleistet werden. Nachdem im Vorfeld eine geeignete Projektstruktur ausgewählt wurde, bedarf es der Abstimmung der Projektmeilensteine. Es ist wichtig, realistische und realisierbare Zeitfenster und Ziele zu wählen. Abgeschlossen wird die Initialisierungsphase mit dem Kick-Off zur DSGVO.

Ergebnis: Initialisierungsphase

- Thema DSGVO evaluiert
- Geeignete Projektstruktur festgelegt
- Kommunikationswege benannt
- Dokumentationsstruktur abgestimmt
- Meilensteine festgelegt
- Projektplan erstellt
- Kick-Off durchgeführt

1. Plan: Aufbau eines Managementsystems

Die Planungsphase beschäftigt sich grundsätzlich damit, die jeweilige Ausgangssituation zu evaluieren. In dieser werden die Ziele des Projektvorhabens formuliert und die Anforderungen an Prozesse, die Organisation und IT aus DSGVO Sicht identifiziert. Ebenso wird in dieser Phase eine Analyse der Ist-Situation mit Hilfe einer GAP-Analyse durchgeführt. In dieser wird geprüft, inwieweit datenschutzrechtliche Anforderungen bereits umgesetzt sind und welche Prozesse, Informationen und Dokumente (Richtlinien, Konzepte usw.) bereits existieren. Wie auch beim ISMS bedarf es eines Risikomanagements. Risiken im Bereich der DSGVO müssen identifiziert und anhand ihres Risikowertes priorisiert werden. Des Weiteren bedarf es einer konkreten Planung und Definition von Maßnahmen sowie einer Sensibilisierung der Mitarbeiter. Eine Hilfestellung für eine konkrete Planung von Schulungsinhalten liefert u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder externe Fachexperten. Letzten Endes müssen alle Aufwendungen und Kosten abgeschätzt und in den Umsetzungsplan übernommen werden.

Ergebnis: Plan-Phase

- GAPs identifiziert
- Status quo ermittelt
- Sensibilisierung geplant
- Risikomanagement etabliert
- Risiken priorisiert
- Umsetzungsplan erstellt

2. Do: Implementieren eines Datenschutz- Managementsystems nach DSGVO

Nach der Durchführung sämtlicher Analysen und der Feststellung der GAPs erfolgt die Umsetzung der zuvor festgelegten Maßnahmen und Ziele. Dabei ist es im Vorfeld wichtig, den Umsetzungsplan an die Projektbeteiligten zu kommunizieren und alle Änderungen nachvollziehbar zu dokumentieren. Dies bedeutet im Detail folgendes: Alle Maßnahmen und Ziele müssen anhand der DSGVO ausgerichtet werden. Es ist möglich, dass ggf. bestehende Prozesse, in denen Abweichungen zur DSGVO festgestellt wurden, überarbeitet werden müssen. Auch müssen neue Prozesse implementiert werden, wie bspw. jene zum Aufspüren oder Löschen personenbezogener Daten.

Benötigte Prozesse und Verfahren nach DSGVO

- Ermittlung von Datenschutzverletzungen
- Aufspüren von personenbezogenen Daten
- Fristgerechtes löschen personenbezogener Daten
- Bearbeitung von Anfragen Betroffener
- etc.

Neben der Einführung neuer Prozesse und Verfahren bedarf es ggf. auch einer Überprüfung bestehender IT-Systeme, welche personenbezogene Daten verarbeiten oder speichern. Werden Produkte verwendet, die ebenfalls personenbezogene Daten speichern oder verarbeiten, muss hier ggf. auch eine Anpassung vorgenommen werden. Abgesehen von Änderungen an technischen Systemen bedarf es auch einer Adaption im Vertragsmanagement. Wurden in der Planungsphase Abweichungen aus datenschutzrechtlicher Sicht festgestellt, müssen bestehende Verträge überarbeitet werden. Des Weiteren müssen die Mitarbeiter im Hinblick auf die neue DSGVO geschult werden. Dafür wird die entwickelte Herangehensweise aus der vorherigen Phase angewendet. Wichtig ist, dass nach Abschluss dieser Phase alle Vorgaben der DSGVO umgesetzt und etabliert wurden.

Ergebnis: Do-Phase

- Maßnahmen umgesetzt
- Schulungen durchgeführt
- Managementsystem aufgestellt

3. Check: Überprüfen und überwachen

Zur stetigen Verbesserung des Datenschutzmanagementsystems bedarf es einer regelmäßigen Überprüfung der umgesetzten Maßnahmen und Prozesse. In Bezug auf die DSGVO gibt es hier keine Vorgabe, in welchen Zeitabständen diese Überprüfung durchgeführt werden muss. Als Fachexperten empfehlen wir jedoch diese einmal in Jahr durchzuführen. Es wird empfohlen einen Prozess zur regelmäßigen Prüfung zu etablieren. Grundsätzlich kann eine Überprüfung der IT-Systeme durch die Durchführung von Penetrationstests erfolgen. Außerdem ist eine Simulation bestimmter Vorfälle denkbar. Es sollte ebenfalls überprüft werden, ob die entwickelten Leit- und Richtlinien bestimmten Vorfällen standhalten können. In Art 24 DSGVO wird darauf aufmerksam gemacht, dass der Verantwortliche unter Berücksichtigung des Kontextes und des Risikos Maßnahmen planen, umsetzen, dokumentieren, prüfen und bei Bedarf verbessern muss. Dies verpflichtet eine Organisation so gesehen zu einer regelmäßigen Überprüfung. Gleichzeitig reduziert eine regelmäßige Überprüfung das Risiko eines Datenschutzverstoßes.

Ergebnis: Check-Phase

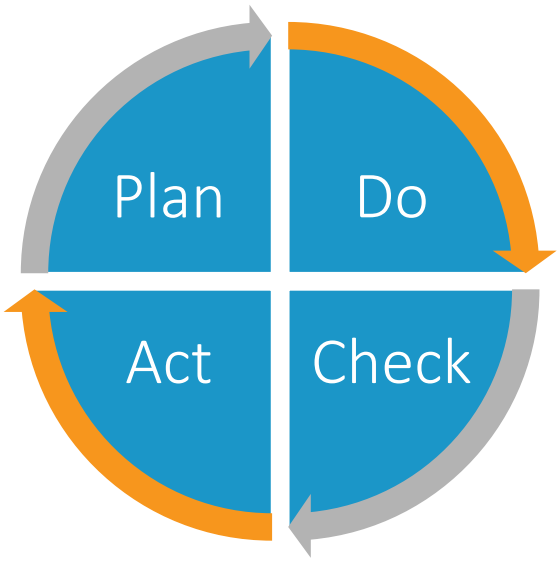
- Einhaltung der DSGVO wird gewährleistet
- Steigerung der Resilienz

4. Act: Optimierung

Liefert Phase drei das Ergebnis, dass z. B. Richtlinien, Ziele oder Maßnahmen modifiziert, zurückgenommen oder ersetzt werden müssen, so wird dies in dieser abschließenden Phase durchgeführt. Im PDCA-Zyklus bildet die Phase der Optimierung und Mängelbeseitigung die letzte Phase, um ein geschlossenes Modell der stetigen Verbesserung zu bilden. Ist diese Phase abgeschlossen, so beginnt der Kreislauf erneut mit der „Plan“-Phase.

Ergebnis: Act-Phase

- Stetige Verbesserung
- Festigung des Managementsystems



Ziele des Managementsystems

Durch die Einführung eines Datenschutz-Managementsystems kann generell eine Reduzierung der Eintrittswahrscheinlichkeit von Datenschutzverstößen gewährleistet werden. Durch die im Managementsystem fest verankerte Risikoanalyse werden mögliche Risiken und Schäden aufgezeigt und behandelt. Kommt es dennoch zu einem Datenschutzverstoß, so können durch die im Vorfeld etablierten Risikoprozesse geeignete Maßnahmen ausgeführt werden, um den Schaden auf ein Minimum zu reduzieren. Des Weiteren reduziert sich das Risiko für betroffene Personen. Neben den genannten Punkten liefert ein Managementsystem für Datenschutz den Nachweis einer datenschutzkonformen Umsetzung der DSGVO. Dies stärkt nicht nur das Vertrauen von Kunden sondern auch von Geschäftspartnern. Gleichzeitig können Bußgelder vermieden bzw. ein Vorwurf der Fahrlässigkeit entkräftet werden. Auch ist eine Integration in bestehende Managementsysteme wie ISO9001 oder ISO27001 problemlos möglich.

Über die Autoren

Bernhard Borsch ist Senior Security Consultant bei der mVISE AG und verantwortet den Bereich Security. Zu seinen Kernkompetenzen zählen neben PKI, Kryptographie, Mobile Security auch das Themenfeld Enterprise Security.

Sebastian Werner arbeitet als Security Consultant bei der mVISE AG. Zu seinen Kernkompetenzen zählt unter anderen die Entwicklung moderner Sicherheitskonzepte auf Basis von ISO27001 und IT Grundschutz.

Was bietet die mVISE an?

Als professioneller Dienstleister mit den Kernkompetenzen in den Bereichen Mobility, Virtualization und Security haben Sie mit der mVISE AG einen starken Partner an Ihrer Seite. Wir unterstützen Sie dabei, den Anforderungen der DSGVO gerecht zu werden. Gemeinsam mit Ihnen entwickeln wir für Sie die beste Lösung für Ihr Unternehmen. Unsere Experten verfügen über Know-How aus verschiedenen Branchen und Unternehmensgrößen. Gleichzeitig profitieren Sie aus unseren umfassenden Erfahrungen in den Bereichen der technischen als auch der organisatorischen IT-Security. Zudem können wir Ihnen umfangreiche Penetrationstests und diverse Workshops zu aktuellen Security bieten.

Ansprechpartner
Bernhard Borsch
Team Lead Security, mVISE AG
Mail: bernhard.borsch@mvise.de
Mobil: +49 152 34151236

Sebastian Werner
Security Consultant, mVISE AG
Mail: sebastian.werner@mvise.de
Mobil: +49 152 03495297