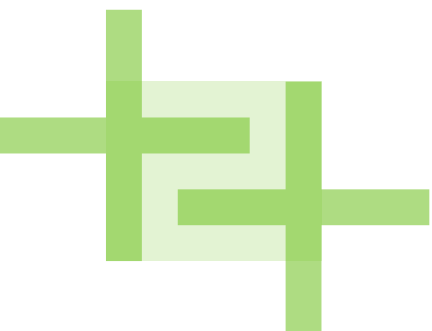
zweiplus

HANDREICHUNG

EU - Datenschutzgrundverordnung (DSGVO)

Verordnung (EU) 2016/679



Übersicht

1. Warum professioneller Datenschutz unerlässlich ist!

Gesetzliche Vorgaben schnell erfüllen

- Datenschutz ist europaweit gesetzlich vorgeschrieben. In Deutschland gelten die strenge Datenschutzbestimmungen, welche im Bundesdatenschutzgesetz (BDSG) und seit 25.05.2018 in der DSGVO geregelt sind. Dabei muss sich jedes Unternehmen - unabhängig von dessen Größe - an die Vorgaben halten.

Kundenanforderungen erfüllen

- Kunden erwarten heute, dass ihre Daten bei Ihnen sicher sind und nach gültigem Recht verarbeitet werden. Durch das Internet sind immer mehr Kunden über ihre Rechte informiert und möchten diese gewahrt sehen. Verstöße gegen Gesetze werden immer häufiger angezeigt.

Grundrechte und Image bewahren

- Bereits im Grundgesetz (GG) wird das Recht auf informationelle Selbstbestimmung formuliert. Niemand möchte darauf verzichten und somit auch keine unberechtigte oder ungeschützte Weitergabe seiner Daten. Für viele Unternehmen steht sonst das eigene Image auf dem Spiel.

Haftungsreduktion und Imageschutz

- Die Einhaltung des Datenschutzes vermindert die Risiken von Geldbußen bis zu 300.000 € bzw. 20Mio in der DSGVO sowie Strafen aus der persönlichen Haftung von Geschäftsführung und Unternehmensleitung. Weiterhin werden die Auswirkungen von Imageschäden z.B. bei Datenpannen reduziert.

Risiko- und Qualitätsmanagement

- Die Umsetzung von Datenschutz und Datensicherheit sind zentrale Bestandteile des unternehmenseigenen Risikomanagementprozesses sein und werden auch im Rahmen von Qualitäts-management-Zertifizierungen (z.B. nach ISO 9001) durch Auditoren geprüft.

Prozessoptimierung

- Durch die Definition und Analyse von Geschäftsprozessen kann neben der Einhaltung des Datenschutzes (z.B. technische und organisatorische Maßnahmen, Löschfristen, etc.) auch eine Optimierung der Prozesse als Synergieeffekt entstehen.

Organisations- und Beschäftigtenschutz

- Durch jährliche Sensibilisierung/Schulung der Mitarbeiter für die Anforderungen des Datenschutzes und der Datensicherheit werden Schwachstellen im Unternehmen früher entdeckt und beseitigt. Mitarbeiter entwickeln ein Eigeninteresse am Schutz der Daten und des Unternehmens.

2. Ziele und Reichweite der Datenschutzgrundverordnung (DSGVO)

- Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

- Die DSGVO gewährleistet die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

- Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

3. Sachlicher Anwendungsbereich (Art. 2 DSGVO)

- Die DSGVO regelt die Verarbeitung personenbezogener Daten, sowohl automatisiert als auch nichtautomatisiert in Dateisystemen (z.B.: auf Servern automatisiert oder in dem Personalordner im Schrank nichtautomatisiert) innerhalb der europäischen Union.

- (Sie gilt nicht für Aktivitäten außerhalb des Anwendungsbereichs der EU-Gesetzgebung, für bestimmte staatliche Tätigkeiten oder für private Nutzung. Sie betrifft auch nicht die Verarbeitung durch Behörden im Zusammenhang mit Strafverfolgung oder öffentlicher Sicherheit. Für die Datenverarbeitung durch EU-Organe gilt eine separate Verordnung. Die Bestimmungen der Verordnung 2000/31/EG über die Verantwortlichkeit von Vermittlern bleiben unberührt.)

- Des weiteren gilt die DSGVO für die Verarbeitung persönlicher Daten, die in EU-Niederlassungen von Unternehmen erfolgt, egal ob die Daten innerhalb oder außerhalb der EU verarbeitet werden. Sie gilt auch für Daten von Personen in der EU, die von Unternehmen außerhalb der EU verarbeitet werden, wenn diese Personen in der EU leben und entweder Waren oder Dienstleistungen angeboten bekommen oder ihr Verhalten in der EU beobachtet wird. Und sie gilt für die Verarbeitung von Daten durch Unternehmen außerhalb der EU, wenn dies in einem Land geschieht, das nach internationalem Recht einem EU-Mitgliedsstaat unterliegt.

4. Pflicht zur Umsetzung der Datenschutzgrundverordnung

- Jegliche erhebende Stelle, die personenbezogene Daten gemäß Art.2 DSGVO verarbeitet
    - Jede Form von Unternehmen
    - Öffentliche Stellen
    - Städte und Kommunen
    - Vereine
    - Kindergärten, Schulen, Technische Hochschulen, Universitäten
    - Senioren- und Pflegeheime

5. Wer muss einen Datenschutzbeauftragten bestellen?

- Alle unter Punkt 4 genannten erhebenden Stellen, die mindestens 20 Beschäftigte haben, welche mit der Verarbeitung personenbezogener Daten betraut sind.
- Als Beschäftigte gelten auch Minijobber, Praktikanten, Studierenden und Auszubildende
- Sofern die erhebende Stelle Daten gemäß Art. 9 DSGVO verarbeitet, so ist stets ein Datenschutzbeauftragter zu bestellen. Die trifft für folgende Bereiche/Branchen zu:
    - Heilberufe
    - Pflegedienste, Senioren- und Pflegeheime
    - Öffentliche Stellen
    - Städte und Kommunen
    - Schulen, Kindergärten, Hochschulen, Universitäten
    - Finanz- und Versicherungsunternehmen gemäß MaRisk/Bafin

6. Rechtlicher Werdegang

- Beschlussfassung der Datenschutzgrundverordnung (DSGVO) durch die EU: Mai 2016

  → 2-jährige Übergangsphase

- Nationale Umsetzung der DSGVO ab 25.05.2018 verpflichtend
- Seit 25.05.2018 ist ein neues Bundesdatenschutzgesetz (BDSG) ergänzend zur DSGVO in Kraft, um die landesspezifischen Besonderheiten zu regeln.
- Seit 01.12.2021 ist das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) ebenfalls ergänzend zur DSGVO in Kraft.
- Am 13.05.2024 wurde das TTDSG in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) umbenannt, um das nationale Gesetz an den europäischen Digitalen Service Act (DSA) anzupassen.
- Am 14.05.2024 wurde das Telemediengesetz (TMG) außer Kraft gesetzt und durch das Digitale-Dienste-Gesetz (DDG) ersetzt.

7. Interne versus zweiplus Umsetzung der DSGVO

	Interner DSB	**zweiplus DSB**
Stellung im Unternehmen	Aufgaben des DSBs oft als Zusatzaufgabe	Neutrale Position im Unternehmen, oft bessere Akzeptanz beim Betriebsrat
Benennung	Oftmals Interessenskonflikte	Unabhängige Benennung
Einarbeitung	Betriebsabläufe sind oft bekannt, Einarbeitung in Prozesse anderer Abteilungen ggf. nötig und Risiko für Betriebsblindheit	Einarbeitung in Betriebsabläufe nötig, aber nimmt objektive, neutrale Perspektive ein, kein Risiko für Betriebsblindheit
Kündigung	Umfangreicher Kündigungsschutz (ähnlich Betriebsrat)	Vereinbarung regulärer Kündigungsfristen über Vertrag
Kosten	Unternehmen finanziert Kosten für Gehalt, Ausbildung, Fortbildungen, Literatur,	Transparente und planbare Kosten durch vertragliche Vereinbarung

	Hardware und Software selbst	
Praxiserfahrung	Begrenzte Praxiserfahrung im eigenen Unternehmen	Fachkunde, große Praxiserfahrung durch Beratung vieler Unternehmen
Zusatzkompetenzen	Oft nur Fachwissen auf einem Gebiet (Datenschutzrecht oder IT-Sicherheit)	Interdisziplinäre Kompetenzen: Datenschutzrecht, IT-Sicherheit, weitere Gesetze wie BDSG, UWG, TDDDG, DDG, HinSchG, betriebswirtschaftliche Kenntnisse, Prozessberatung und Erfahrung in Begleitung von Veränderungsprozessen
Netzwerk	Wenig Netzwerk vorhanden	Mitglied in Vereinigungen für Datenschutzbeauftragte, gut vernetzt mit anderen Experten
Unabhängigkeit	Festangestellte Beschäftigte, die in betrieblichen Regelprozessen eingebunden sind, können faktisch nicht weisungsfrei handeln.	Unabhängig und weisungsfrei, keine Hemmungen Probleme anzusprechen sowie ausschließliche Konzentration auf Datenschutz
Akzeptanz im Unternehmen	Ein regulär Beschäftigter könnte möglicherweise nicht vollständig in eine Stabsstelle integriert werden, die weitgehend unabhängig von direkter Anleitung arbeitet.	Unabhängige Stellung, externer DSB wird anders wahrgenommen und füllt weisungsfreie Stabsstelle adäquat aus
Arbeitsaufwand	Oft stehen für die Tätigkeit als interner Datenschutzbeauftragter aufgrund der Hauptaufgaben nur begrenzte Ressourcen zur Verfügung, was einen längeren Einarbeitungszeitraum und einen erhöhten Arbeitsaufwand bedeuten kann.	Für einen externen Datenschutzbeauftragten stehen in der Regel bessere Ressourcen zur Verfügung und der Zeitbedarf für Einarbeitung ist geringer und somit effizienter im Vergleich zu internen Datenschutzbeauftragten, da sie auf ihre Kernkompetenzen fokussiert sind und nicht von anderen internen Aufgaben abgelenkt werden.
Zeitliche Verfügbarkeit	Oftmals eingeschränkt durch andere Aufgaben	Immer verfügbar, kurze Antwortzeiten

8. zweiplus DSGVO-Gesamtlösung

- Wir bilden für Sie 100 % der Anforderungen zur Umsetzung der DSGVO ab
- Bereitstellung eines sicheren DSMS (Datenschutzmanagementsystems (365/7/24))
- Begleitung des gesamten DSGVO Umsetzungsprozesses
- Stellung mehrerer TÜV-zertifizierter Datenschutzbeauftragter
- Sichere Kommunikation über das DSMS
- Sofortige Anpassung der Prozesse und des DSMS an sich ändernde Gesetzeslagen
- Transparente Kosten durch ein **Festpreismodell, keine versteckten Kosten**
- Entlastung interner Ressourcen
- Zertifiziert durch einen akkreditierten Datenschutz-Auditor TÜV

9. zweiplus Vorgehensweise zur Umsetzung der DSGVO

- Initialisierung
    - Entwurf grober Zeitplan, Ressourcen
    - Zuständigkeiten/Verantwortliche bestimmen
    - Erhebung des aktuellen Datenschutzniveaus / vorhandene Dokumentationen
    - Organisation, IT-Infrastruktur im Überblick erfassen
    - Schulungs- und Sensibilisierungsmaßnahmen der Beschäftigten festlegen
    - Einführung des DSMS (Datenschutzmanagementsystem)

- Verzeichnis der Verarbeitungstätigkeiten (VVT)
    - IT-Inventarisierung (Hard- und Software)
    - Verantwortliche/Ansprechpartner der einzelnen Fachbereiche identifizieren
    - Verfahren zur Risikoanalyse einbeziehen
    - Wenn Verfahrensverzeichnis nach BDSG bis 2018 vorhanden, prüfen und überführen in VVT
    - wenn nein, VVT neu erfassen
    - VVT als Auftragsverarbeiter erforderlich? Wenn ja, erstellen

- Datenschutz-Folgenabschätzung (wenn notwendig)
    - Prüfsystem erstellen und etablieren
    - VVT mit hohem Risiko vorhanden? Risikoanalyse erfolgt in VVT
    - Folgenabschätzung durchführen

- Datenschutz in Vereinbarungen
    - Dienstleister identifizieren
    - Vorhandene Verträge prüfen
    - Neue Verträge erstellen

- Privacy by Design & Default
    - Datensicherheit und -schutz durch Technik und datenschutzfreundliche Voreinstellungen (Stand der Technik)
    - Technische und organisatorische Maßnahmen aufnehmen, falls nicht vorhanden
    - Umsetzung technischer und organisatorischer Maßnahmen anhand jeweiligem Risikoprofil

- Betroffenenrechte
    - Auskunftsrecht
    - Berichtigung / Löschung
    - Einschränkung
    - Datenübertragbarkeit
    - Widerspruchsrecht

- Umgang mit Datenschutzvorfällen
    - Etablierung einer Vorgehensweise im Falle von Datenschutzvorfällen
    - Meldepflichten
    - Dokumentationspflichten