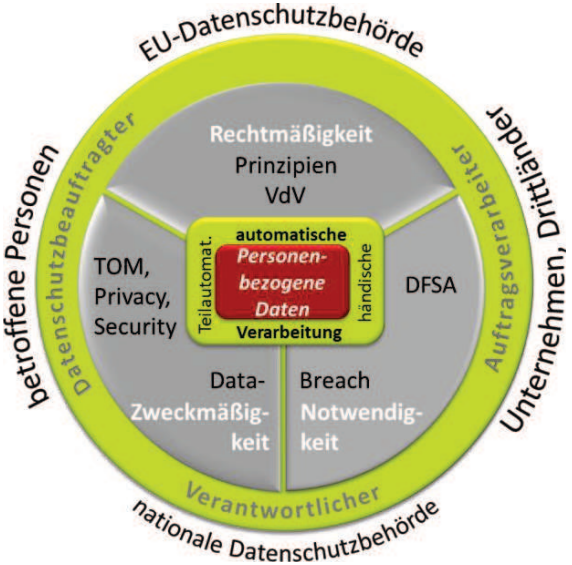
DSGVO leicht erklärt

Pflichten, Rechte, Chancen und Risiken durch die neue Datenschutzgrundverordnung (DSGVO)



Wir stehen erst am Beginn der Digitalisierungsepoche. Nutzen Sie die Chancen der DSGVO. Nichts Tun ist keine Option!

Fragenstellungen und erste Orientierung (roter Faden)

Nachfolgend eine Übersicht, welche zentralen Fragen im Buch behandelt werden. Das Ziel des vorliegenden Buches ist, dass jeder Leser Handlungsoptionen ableiten und weiterführende Entscheidungen zur Handhabung der DSGVO treffen kann.

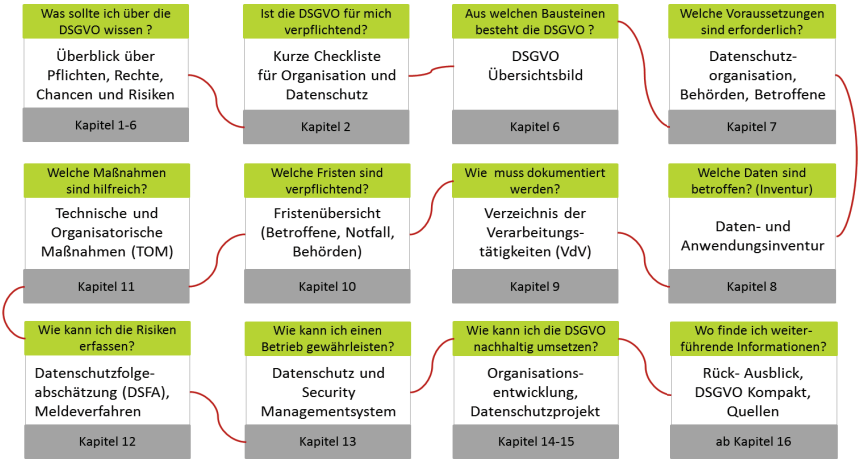


Abbildung 1: Fragen und Themen der DSGVO

Das Werk soll Unternehmer, Organisationsverantwortliche und Interessierte dabei unterstützen, die DSGVO in ihrer Gesamtheit zu verstehen und anwenden zu können. Der Schwerpunkt liegt nicht, wie bei den meisten DSGVO Publikationen auf dem rechtlichen Teil, sondern im Grundverständnis und in der pragmatischen Anwendbarkeit. Die Kapitel folgen einem roten Faden und haben keinen Anspruch auf juristische Vollständigkeit.

Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige beider Geschlechter.

Weiterführende Informationen/Referenzen: http://www.mayr-consulting.at/

Rückfragen und Empfehlungen sind durchaus erwünscht.

Inhalt

Abbildungsverzeichnis

1. Vorwort

Durch die Digitalisierungswelle boomen neuartige Geschäftsmodelle auf Basis persönlicher Daten. Das Ziel der DSGVO: „Der Bürger soll Herr seiner Daten sein, nicht die Datenindustrie! “

Die EU und deren Mitgliedsländer haben sich dieser Dynamik angenommen. Mit 25. Mai 2018 tritt nach einer 2-jährigen Übergangsfrist die erste EU-weite Datenschutzgrundverordnung (DSGVO) in Kraft. Die DSGVO regelt europaweit den Umgang mit personenbezogenen Daten. Das Strafausmaß (bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes) für eine Verletzung der DSGVO kann sehr schmerzhaft sein und bis zur Stilllegung der Datenverarbeitung führen. Kommt es zu einer Beschwerde eines Betroffenen bei der Datenschutzbehörde (DSBh), muss die Organisation die Einhaltung der DSGVO nachweisen. Kann sie das nicht, kann bereits EIN Vorfall zur Überlebensfrage werden.

Klingt bedrohlich – muss es aber nicht sein!

Dennoch stellen sich für große wie kleine Unternehmen, Vereine, Ngos die Fragen:
In welcher Art und Weise bin ich betroffen? Was muss ich konkret tun, damit ich die Anforderungen zielorientiert und wirtschaftlich erfüllen kann? Womit fange ich am besten an?

Das Ziel des Buches ist, das DSGVO-Konzept einfach und nachvollziehbar zu vermitteln. Denn nur wenn die DSGVO prinzipiell verstanden wurde, können sich zukunftsorientierte Handlungsoptionen entwickeln.

Neben den viel zitierten Pflichten und Rechte ergeben sich durch die DSGVO ebenso eine Vielzahl von bis dato eher spärlich dokumentierte Chancen. Um diese Chancen in der gesamten Wertschöpfungskette nutzen zu können, braucht es eine pragmatische Organisationsentwicklung. In diesem Werk wird aufgezeigt, wie die DSGVO Pflichten und Rechte in Organisationen, in deren Strukturen und Abläufe machhaltig eingeführt und die damit einhergehenden Chancen genutzt werden können. Die rechtliche Konformität, sowie die technische Datensicherheit werden als „Qualitätssicherungsmaßnahmen“ sowohl in der Einführung wie auch in der täglichen Praxis betrachtet.

Anhand eines praxisorientierten Übersichtsmodells werden die wesentlichen Bausteine und Rollen der DSGVO vermittelt und mit Beispielen erläutert. Die daraus resultierende Vorgehensweise, soll Unternehmen, Vereine und NGOs in ihrer autonomen Handlungsfähigkeit unterstützen die kontinuierliche Weiterentwicklung anhand des bewährten Deming-Lifecylce „Plan-Do-Check-Act“ umzusetzen. Zu guter Letzt werden noch Links z.B. zur EU-DSGVO, Datenschutzbehörde uvm. angeführt.

Sie werden erstaunt sein in welcher kurzer Zeit Sie über ein umfassendes DSGVO Wissen verfügen.

Viel Freude und Klarheit beim Lesen.

Gerald Mayr

2. Pflichten aus der DSGVO

Die aus dem Jahre 1995 von der Europäischen Gemeinschaft erlassene Datenschutzrichtlinie zur Verarbeitung personenbezogener Daten (Richtlinie 95/46/EG) wird am 25. Mai 2018 von der EU Datenschutz-Grundverordnung (DSGVO) mit dem Ziel abgelöst, einen einheitlichen Datenschutz zur Verarbeitung von personenbezogenen Daten in Europa zu gewährleisten. Nationale Anpassungen, sogenannte Öffnungsklauseln sind teilweise möglich.

Je nach Größe der Unternehmen bzw. Art der verwendeten Daten und damit verbundenen Risiken, ergeben sich eine Vielfalt von Verpflichtungen. Dies beginnt bei der Rechenschafts- und Dokumentationspflicht, beim Führen eines Verarbeitungsverzeichnisses, der Verpflichtung zur Datenschutz-Folgenabschätzung, besondere Meldepflichten im Zusammenhang mit Verletzungen des Datenschutzes (Data Breach, Privacy by Design, Default), Pflicht zur Überprüfung der Wirksamkeit von Datensicherheitsmaßnahmen, Auskunftspflicht für Betroffene bis hin zur verpflichtenden Bestellung eines Datenschutzbeauftragten um einige Pflichten konkret anzuführen.

2.1. EU-Rechtsrahmen

Die DSGVO stellt einen Rechtsrahmen dar, der für alle EU-Staaten gleichermaßen gilt. Der Rechtsrahmen gilt für alle Unternehmen die in der EU ansässig sind als auch für jene die Dienstleistungen und Produkte in der EU anbieten. Bei einer Datenverarbeitung durch Unternehmen welche außerhalb der EU ansässig sind, ist besonders darauf zu achten, dass eine Anerkennung der DSGVO Regelungen in demselben Umfang vertraglich sichergestellt ist (Datenschutzniveau).

2.2. Nationale Anpassungen (Öffnungsklausel)

Seitens der EU wurde den Mitgliedsländern in bestimmten Punkten Anpassungen (z.B. verpflichtender Datenschutzbeauftragter) bzw. Anpassungen durch sogenannte Öffnungsklauseln zu erstellen, eingeräumt. In zentralen Punkten wie z.B. Regelungen zur Datenweiterleitung und Bußgeldern trifft dies nicht zu. Damit sollen strategische Überlegungen, wie Standortwechsel in sogenannte Bußgeld-Billigländer von Beginn an ausgeschlossen werden. Österreich versucht aktuell eine Abschschwächung im Nationalrat zu erwirken.

2.3. Zielsetzung der DSGVO

Der Bürger soll Herr seiner Daten sein, nicht die Datenindustrie! Der Schutz personenbezogener Daten ist ein wichtiges Persönlichkeitsrecht jedes Einzelnen.

Zielsetzungen der DSGVO sind

- einheitlicher Rechtsschutz für alle Betroffenen in der EU.
- einheitliche Regeln für die Datenverarbeitung von personenbezogenen Daten innerhalb der EU.
- Gewährleistung eines starken und einheitlichen Vollzuges.

Aus diesen Zielsetzungen resultieren gegenüber der aktuellen Datenschutzrichtlinien 95/46/EG neue Verpflichtungen und Rechte.

Abbildung 2: Verpflichtungen und Rechte

Aus den neuen Pflichten und den damit eingehenden Rechten für natürliche Personen, ergibt sich die Konsequenz, die betroffenen Personen besser kennenzulernen. Das Vertrauen in die Menschen wird zunehmend in den Vordergrund gestellt. Eine Chance für kundenorientierte Organisationen.

2.4. Ein erster praktischer Einblick

Das Hauptziel der neuen EU-DSGVO besteht darin, die Privatsphäre und den Schutz personenbezogener Daten von betroffenen Personen zu gewährleisten. Betroffene Personen sollen in der Lage sein, die Datenverarbeitung (Daten-Lebenszyklus: Erhebung, legitime Verarbeitung, Weitergabe, Löschung) ihrer persönlichen Daten steuern zu können.

Die verarbeitenden Unternehmen, Organisationen, Vereine, NGOs, öffentliche Stellen, Behörden (in weiterer Folge Organisationen benannt) werden durch die DSGVO verpflichtet bei Anfrage von Betroffenen diese innerhalb eines bestimmten Zeitraums zu bearbeiten. Erfolgt dies nicht, kann der Betroffene bei der Behörde eine Beschwerde einreichen. Die Behörde ist verpflichtet innerhalb von 3 Monaten den Betroffenen über den Stand der Ermittlungen zu informieren.

Kommt es bei den verarbeitenden Organisationen zu einer Datenschutzverletzung, muss unmittelbar bzw. bis spätestens 72 Stunden nach Eintritt der Verletzung eine Meldung an die Behörde erfolgen. Wenn Gefahr für die Privatsphäre droht, bzw. efolgt eine Anordnung der Behörde muss der Betroffene ebenso informiert werden.

In beiden Fällen muss die Organisation nachweisen, dass die DSGVO ordnungsgemäß umgesetzt und gelebt wird (Rechenschaftspflicht).

Dazu muss die Organisation ein Verzeichnis aller Verarbeitungstätigkeiten führen (anstatt der Meldepflicht im DSG 2000) und darin alle zweckgebundenen Verarbeitungstätigkeiten dokumentieren. Auf Basis des Verarbeitungsverzeichnisses erfolgt die Risikoabschätzung (Datenschutzfolgeabschätzung) und die daraus resultierenden Datenschutzvorkehrungen (Datenschutz durch Technik und Voreinstellungen bzw. Privacy by Design, Privacy by Default), sowie die technischen und organisatorischen Maßnahmen zur Risikominimierung.

Grundsätzlich müssen für alle Datenverarbeitungen zweckgebundene Einverständniserklärungen von betroffenen Personen, oder gesetzlichen Vertretern bei Kindern, vorab eingeholt werden. Auf Verlangen der Behörde muss die ordnungsgemäße Einhaltung der DSGVO Datenschutzgrundsätze (Prinzipien) nachgewiesen werden können (z.B. Dokumentation, regelmäßige Audits, Datenschutz Managementsystem, Zertifizierungen). Diese Anforderungen bestehen auch für die Einbeziehung von zusätzlichen Auftragsverarbeitern (Dienstleistern), die bei der Erfüllung des Verarbeitungszweckes mitwirken (Datenweiterleitung).

Den Behörden wurden dazu umfangreiche Kompetenzen und Mahnmöglichkeiten (Bußgelder bis zu 20 Millionen € bzw. 4 % des Vorjahresumsatzes) mit dem Ziel eingeräumt, den Datenmissbrauch in allen EU-Ländern einheitlich zu unterbinden. Eine wichtige und längst fällige Antwort auf die dynamischen Entwicklungen der Digitalisierung und der damit einhergehenden globalen Datenindustrie.

Der Verantwortliche einer Organisation (Geschäftsführer, Unternehmensleiter, Präsident) ist rechtlich verantwortlich. Es ist keine Delegation möglich. Zur Unterstützung der DSGVO Einhaltung kann der Verantwortliche einen internen oder externen Datenschutzbeauftragten bestellen.
Bei bestimmten Voraussetzungen (Unternehmensgröße, Datenkategorie) ist der Verantwortliche gesetzlich dazu verpflichtet. Der Datenschutzbeauftragte vertritt den Verantwortlichen bei Behörden- und Betroffenenanliegen und berät den Verantwortlichen. Er ist jedoch nicht Weisungsgebunden. Die Verantwortung und Haftung bleibt vollends beim Verantwortlichen.

2.4.1. Natürliche, betroffene und juristische Personen

Natürliche Personen bzw. betroffenen Personen nach der DSGVO sind

- Kunden, Mitglieder (Erwachsene, Kinder),
- Mitarbeiter, Lieferanten, Geschäftspartner,
- Auftragsverarbeiter, SUB-Auftragsverarbeiter (vormalig Dienstleister)
- Stakeholder.

Nach der gegenständlichen Formulierung im aktuellen zur Begutachtung eingereichten nationalen Anpassungsgesetzes darf man davon ausgehen, dass die juristische Person weiterhin vom Schutz des Datenschutzgesetzes umfasst ist. Der Fokus liegt jedoch eindeutig auf der natürlichen Person.

2.4.2. Die Dynamik der Digitalisierung erfordert neue Regelwerke

Die großen Internetfirmen wie z.B. Google, Amazon, Facebook haben ihre Geschäftsmodelle auf der Basis von persönlichen Daten aufgebaut und beherrschen dadurch zunehmend die Märkte.
Das Geschäftsmodell ist relativ einfach erklärt. Die Nutzer stellen freiwillig ihre (persönlichen) Daten gegen Gratisnutzung der Software zur Verfügung. Was mit den Daten geschieht, in welchen weiteren Geschäftsfeldern die Daten mitwirken bzw. wo die Daten liegen, kann man bestenfalls erahnen, sofern man sich die Mühe macht die kleingedruckten und oftmals verwirrend geschriebenen AGBs zu lesen. Vom Verstehen mal ganz abgesehen.

2.4.3. Alles hat eben seinen Preis, auch das „Dabei sein".

Für manche Personen stellt diese Vorgehensweise auf den ersten Blick auch kein Problem dar. Setzt man sich jedoch intensiver mit der Thematik auseinander kommen doch einige Fragen zum Vorschein. Was ist, wenn mit den Daten nicht sorgsam umgegangen wird? Wenn Missbrauch oder Datenverlust entsteht? Wenn meine Bankdaten, Versicherungs- und Gesundheitsdaten usw. in falsche Hände kommen? Was bedeutet das für mich, wenn meine Daten ohne mein Einverständnis weiterverarbeitet oder verkauft werden? Was, wenn neue Regierungsformen, neue Informationsdienste, neue Geschäftsmodelle kommen?
Fragen über Fragen. Mit jedem weiteren Gedanken kommen neue „Was wenn" Gedanken.

Faktum ist, dass immer und überall Daten gesammelt werden. Oftmals wissen wir gar nichts davon, wo unsere Daten aufgenommen und gespeichert werden, wie z.B. bei den Videodaten in Einkaufszentren usw. Es ist eine Tatsache, dass in vielen Organisationen wesentlich mehr Daten gesammelt werden, als für den ursächlichen, und hoffentlich zuvor vereinbarten Geschäftszweck notwendig sind (Stichwörter: „Big Data" oder „Big brother is watching you").

2.4.4. Die DSGVO eine logische Konsequenz

Die DSGVO hebt die nationale Datenschutzrichtlinie 2000 auf und wird ab Mai 2018 das Rückgrat des allgemeinen Datenschutzes der EU bilden. Die DSGVO ermöglicht stellenweise „Öffnungs- bzw. Anpassungsklauseln", die den nationalen Gesetzgeber berechtigen bestimmte Angelegenheiten gesetzlich individuell zu regeln. Es kann daher neben der DSGVO weiterhin ein nationales Datenschutzgesetz (Österreich: DSG 2018) geben. Die Bußgelder pro Verstoß sind jedoch EU weit einheitlich.