Inhaltsverzeichnis

1 Einführung 6
- 1.1 Die Datenschutz-Grundverordnung (DSGVO) 7
- 1.2 Das Bundesdatenschutzgesetz (BDSG) 8
- 1.3 Die ePrivacy-Verordnung 8

2 Häufige Fragen und Antworten zum Datenschutz 9
- 2.1 Warum ist Datenschutz notwendig? 10
- 2.2 Wen schützt die Datenschutz-Grundverordnung (DSGVO)? 11
- 2.3 Was sind personenbezogene Daten? 11
- 2.4 Daten von Kindern und Jugendlichen 11
- 2.5 Was sind besondere Kategorien personenbezogener Daten? 11
- 2.6 Was sind die rechtlichen Grundlagen für die Datenverarbeitung? 11
- 2.7 Was bedeutet „Verarbeitung"? 12
- 2.8 Was ist ein „Verantwortlicher" und was macht ein „Auftragsverarbeiter"? 12
- 2.9 Was ist Profiling? 13
- 2.10 Was bedeuten Data Protection by Design und Data Protection by Default? 13
- 2.11 Wann wird ein Datenschutzbeauftragter benötigt? 14

3 Die Datenschutzgrundsätze 15
- 3.1 Rechtmäßigkeit der Verarbeitung 15
- 3.2 Verarbeitung nach Treu und Glauben 16
- 3.3 Transparenz 17
- 3.4 Zweckbindung 17
- 3.5 Datenminimierung 18
- 3.6 Richtigkeit der Datenverarbeitung 18
- 3.7 Speicherbegrenzung, Datenaufbewahrung und Löschung nach DSGVO 18
- 3.8 Integrität und Vertraulichkeit 20
- 3.9 Rechenschaftspflicht (Accountability) 21

4 Der Datenschutzbeauftragte (DSB) und der Datenschutz-Manager (DSM) 21
- 4.1 Die Aufgaben des Datenschutzbeauftragten (DSB) 21
- 4.2 Die Aufgaben des Datenschutz-Managers (DSM) 22

5 Erhebung und Verarbeitung von personenbezogenen Daten 23

6 Die Datenschutzerklärung 23

7 Betroffenenrechte 23
- 7.1 Recht auf Auskunft 24
- 7.2 Recht auf Berichtigung 25
- 7.3 Recht auf Löschung 25
- 7.4 Recht auf Vergessenwerden 26
- 7.5 Recht auf Einschränkung der Verarbeitung 26
- 7.6 Recht auf Datenübertragbarkeit 27
- 7.7 Recht auf Widerspruch 28

8 Weitergabe von Daten 28

9 Auftragsverarbeitung 28

10 Technische und organisatorische Maßnahmen (TOM) 30

11 Verzeichnis von Verarbeitungstätigkeiten 31

12 Die Datenschutz-Folgenabschätzung 32

13 Datenschutzvorfälle und Meldung von Datenschutzverstößen 34

14 Das Datenschutz-Management-System 35
- 14.1 Aufbau und Dokumentation eines Datenschutz-Management-Systems 37
- 14.2 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes 38

15 Die Rolle des Unternehmens und die Konsequenzen 39
- 15.1 Wer trägt die Verantwortung im Unternehmen? 39
- 15.2 Die Konsequenzen 39

16 Regeln zum Datenschutz und zur Datensicherheit 41

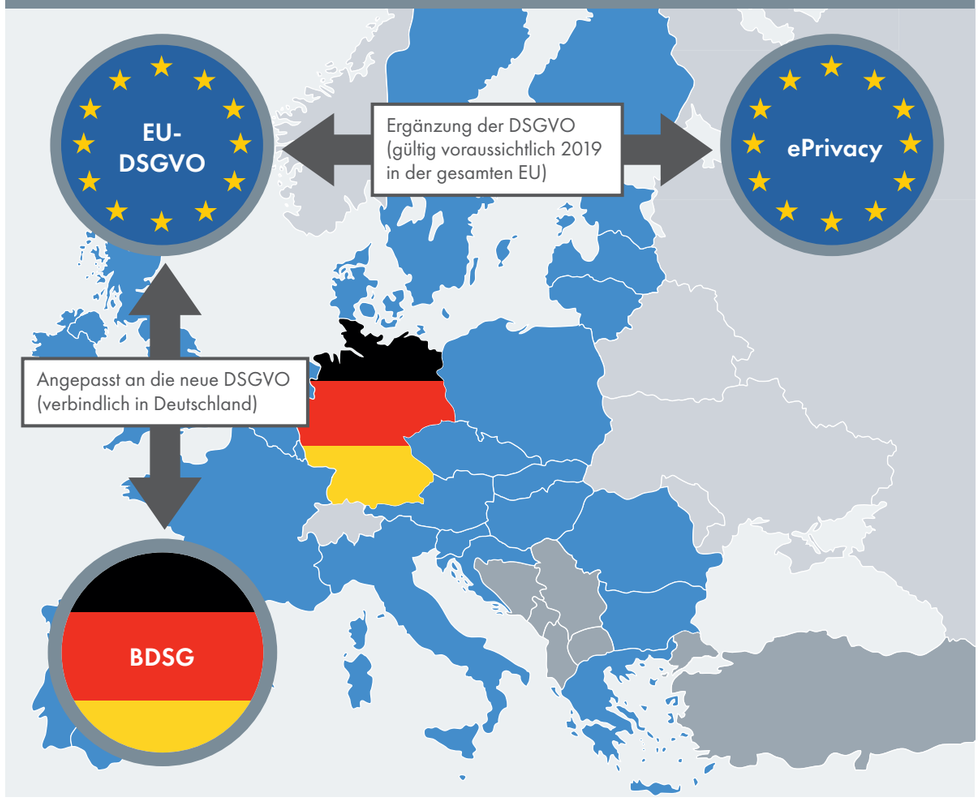
1 Einführung

In der gesamten Europäischen Union gilt seit dem 25. Mai 2018 die Datenschutz-Grundverordnung. Die Abkürzung für diesen langen Namen lautet EU-DSGVO oder auch einfach DSGVO. Das Ziel der Verordnung ist, den Datenschutz in der EU zu modernisieren und zu vereinheitlichen. Ergänzt wird die DSGVO durch ein neues Bundesdatenschutzgesetz (BDSG) und künftig durch die ePrivacy-Verordnung der Europäischen Union.

Diese Informationsbroschüre soll Mitarbeiterinnen und Mitarbeiter in Unternehmen sowie am Datenschutz interessierten Mitmenschen in einfacher und klarer Sprache einen Überblick über die Grundlagen und die Prinzipien des Datenschutzes geben. Sie erklärt, welche Rechte die betroffenen Personen und welche Pflichten die Verantwortlichen haben. Zudem beschreibt sie die Rolle des Datenschutzbeauftragten und die des Datenschutz-Managers in Unternehmen.

Die Datenschutz-Grundverordnung enthält mit 99 Artikeln sowie 173 Erwägungsgründen umfangreiche Regelungen. Auf die Nennung der konkreten DSGVO-Artikel, der Erwägungsgründe sowie auf die Nennung der BDSG-Paragrafen wird in dieser Broschüre absichtlich verzichtet, damit der Text besser lesbar und verständlicher ist.

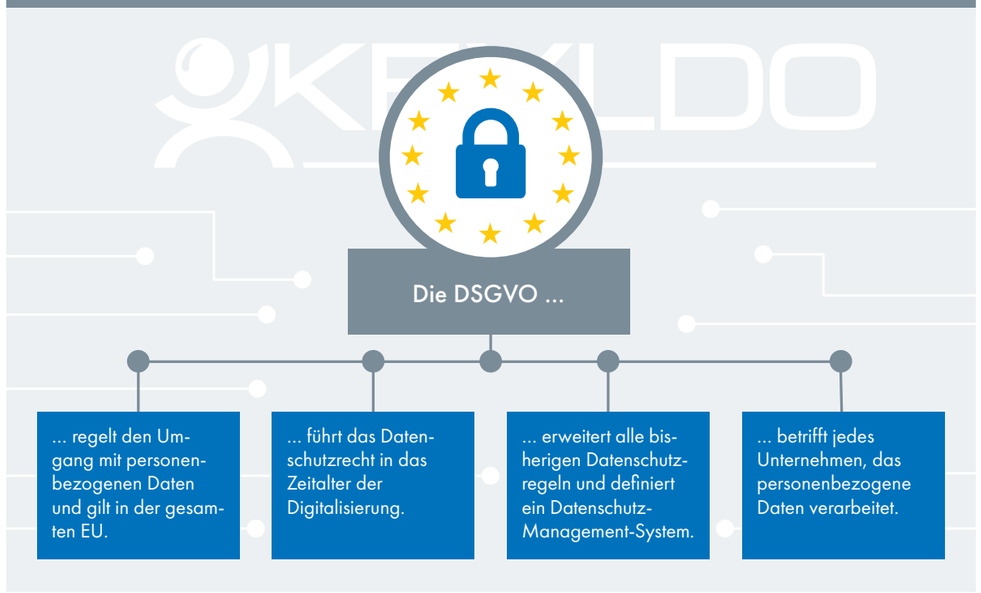
Die maßgeblichen Gesetze zum Datenschutz



© 2019 Keyldo GmbH / Illustration Europakarte: designed by Freepik

Abbildung 1

Warum gibt es die Datenschutz-Grundverordnung?



© 2019 Keyldo GmbH

Abbildung 2

1.1 Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO soll in erster Linie die Grundrechte und die Grundfreiheiten natürlicher Personen schützen. Konkret: Ihr Recht auf den Schutz ihrer personenbezogenen Daten. Und sie soll die Selbstbestimmung des Einzelnen stärken, damit er entscheiden kann, wie mit seinen personenbezogenen Daten umgegangen wird.

Für Unternehmen, die in der Regel personenbezogene Daten verarbeiten, heißt das: Sie müssen damit verantwortlich und sorgfältig umgehen. Dazu gehört auch eine risikobewusste Nutzung von IT-Systemen und -Anwendungen. Die DSGVO enthält zahlreiche Anforderungen an den Schutz personenbezogener Daten. Bei Datenschutzverstößen drohen hohe Geldbußen und Sanktionen.

Das Thema Datenschutz betrifft uns im Alltag in mehrfacher Hinsicht. Unternehmen verarbeiten unsere Daten, weil wir bei ihnen Kunde oder Mitarbeiter sind. Mitarbeiter von Unternehmen verarbeiten personenbezogene Daten von Dritten.

Personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten oder sonstigen Dritten dürfen nur auf Grundlage von gesetzlichen Vorschriften und von entsprechenden internen Anweisungen verarbeitet werden. Die Wahrung der Vertraulichkeit ist eine arbeits- und datenschutzrechtliche Pflicht.

Datenschutz ist eine Managementaufgabe, weil es gilt, Datenschutzverstöße zu vermeiden. Das Management sollte folglich ein hohes Datenschutzniveau sicherstellen. Ziel des Datenschutzes im Unternehmen ist die Etablierung eines Datenschutz-Management-Systems (DSMS), das alle Anforderungen der DSGVO ganzheitlich abdeckt. Wie so ein System aufgebaut und kontinuierlich verbessert werden kann, wird in Kapitel 14 ausführlicher skizziert.

Ein DSMS stellt sicher, dass die Anforderungen an die von der DSGVO geforderte Rechenschaftspflicht erfüllt werden. Rechenschaftspflicht bedeutet in diesem Zusammenhang, dass der Verantwortliche nachweisen und belegen muss, dass er seinen Verpflichtungen zum Datenschutz nachkommt.

1.2 Das Bundesdatenschutzgesetz (BDSG)

Zeitgleich mit der DSGVO trat auch das neue Bundesdatenschutzgesetz (BDSG) in Kraft. Da die DSGVO einige sogenannte Öffnungsklauseln enthält – bestimmte Aspekte, die die einzelnen Länder selbst regeln sollen –, mussten diese vom deutschen Gesetzgeber ausgestaltet werden.

Das BDSG hat 85 Paragrafen. Es ergänzt, konkretisiert und modifiziert die DSGVO. Es beinhaltet beispielsweise spezielle Regelungen für den Beschäftigtendatenschutz, für Scoring und Bonitätsauskünfte, für das Profiling sowie für den betrieblichen Datenschutzbeauftragten.

Das BDSG besteht aus vier Teilen:
- Der erste Teil ist ein allgemeiner Abschnitt.
- Der zweite Teil betrifft die Umsetzung der DSGVO.
- Der dritte Abschnitt betrifft ausschließlich Behörden, die personenbezogene Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung verarbeiten.
- Der vierte Teil betrifft die Verarbeitung personenbezogener Daten, die nicht unter die Regelung der EU fallen.

Ob alle Regeln des neuen BDSG im Streitfall vor Gerichten Bestand haben werden, lässt sich noch nicht abschätzen. Oft ist es ein schmaler Grat zwischen Ausgestaltung und Neuregelung. Unternehmen müssen aktuell darauf vertrauen, dass das BDSG mit der Datenschutz-Grundverordnung in Einklang steht und abwarten, zu welchem Ergebnis die Gerichte in Zukunft kommen werden. Derzeit nimmt das BDSG sowohl Einschränkungen als auch Erweiterungen der DSGVO im Geltungsbereich der Bundesrepublik vor.

1.3 Die ePrivacy-Verordnung

Vereinfacht gesagt, ist die ePrivacy-Verordnung (ePVO) eine Ergänzung der Datenschutz-Grundverordnung (DSGVO). Sie ist als Spezialgesetz innerhalb des EU-Datenschutzrechts angelegt und soll die DSGVO im Hinblick auf elektronische Kommunikationsdaten, die als personenbezogene Daten einzustufen sind, präzisieren und ergänzen.

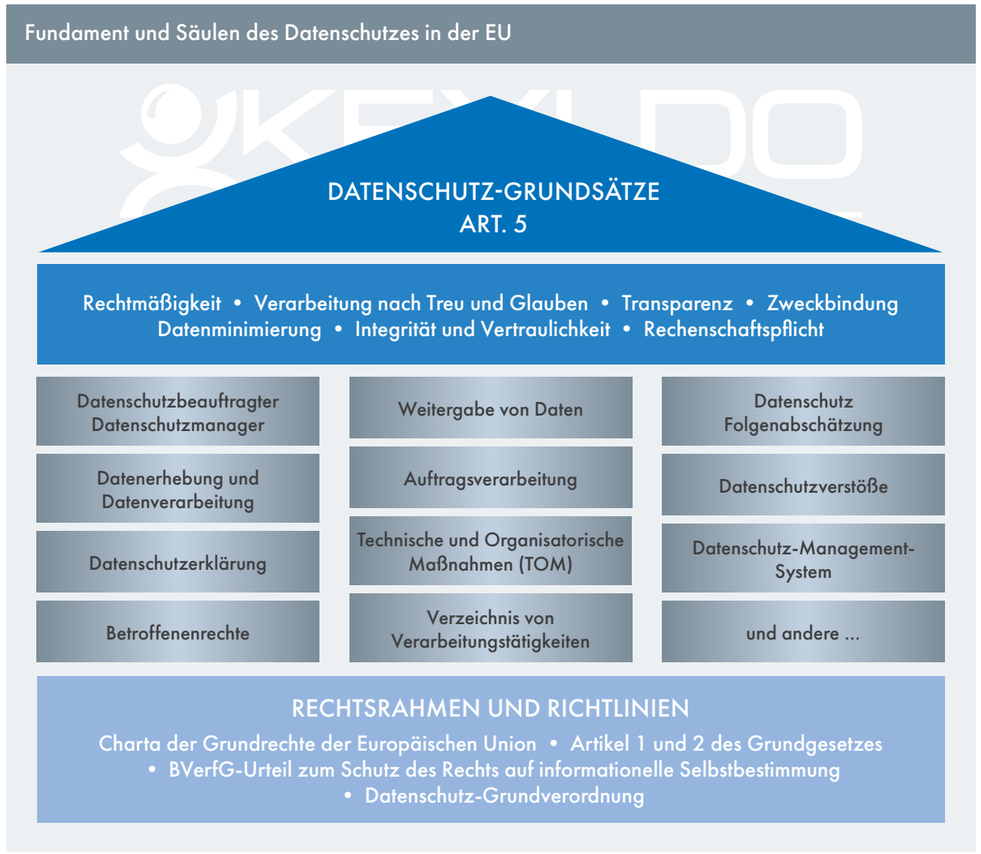
Die ePVO schließt Regelungslücken und definiert neue Vorgaben, die sich auf Grund der technischen Entwicklung ergeben haben. Im Kern geht es bei der ePVO darum, personenbezogene Daten in der elektronischen Kommunikation besser zu schützen und die Sicherheit für die Nutzer zu erhöhen. Während die DSGVO erst ansetzt, wenn personenbezogene Daten vorliegen, geht es in der ePVO darum, was auf dem Weg dorthin passiert, wenn wir elektronische Kommunikationsdienste verwenden.

Vorgesehen ist, dass Vorgaben für die Telekommunikation definiert werden wie:
- Die Anzeige der Rufnummer des Anrufers und des Angerufenen oder deren Unterdrückung sowie Ausnahmen
- Die Sperrung eingehender Anrufe
- Vorgaben für öffentlich zugängliche Verzeichnisse (öffentliche Verzeichnisse der Endnutzer elektronischer Kommunikationsdienste sowie über Auskunftsdienste)
- Unerbetene Kommunikation und Vorgaben für Direktwerbung über elektronische Kommunikationsdienste
- Informationspflichten über erkannte Sicherheitsrisiken
- Aufgaben der Aufsichtsbehörden und Sanktionsmöglichkeiten

Die ePVO wird Regelungen ersetzen, die in Deutschland größtenteils im Telekommunikationsgesetz (TKG) und im Telemediengesetz (TMG) umgesetzt sind. Das Gesetzgebungsverfahren für die ePVO läuft noch (Stand: Anfang 2019). Geplant ist, die ePrivacy-Verordnung 2019 in Kraft treten zu lassen, wobei es wohl eine mindestens einjährige Übergangsfrist geben wird.

2 Häufige Fragen und Antworten zum Datenschutz

Wenn wir Unternehmen beraten und wenn Keyldo-Berater Datenschutz-Seminare durchführen, stoßen wir immer wieder auf ähnliche Fragen. In diesem Kapitel gehen wir darauf ein und beantworten häufige Fragen zum Datenschutz. Als Einführung zeigen wir das „Grundgerüst" der DSGVO. Die folgende Abbildung benennt wichtige Säulen, auf denen die Datenschutz-Grundverordnung aufbaut.



© 2019 Keyldo GmbH

Abbildung 3