



# Schutz personenbezogener Daten und DSGVO



# Inhaltsverzeichnis

<b>1. Einführung .....</b>	<b>6</b>
<b>2. DSGVO .....</b>	<b>7</b>
2.1. Prinzipien der DSGVO .....	8
2.2. Verwendung, Verarbeitung, Speicherung und Übertragung von Daten in der EU .....	9
2.3. Zustimmung zur Datenverarbeitung .....	12
2.4. Recht auf Zugang und Recht auf Datenübertragbarkeit .....	15
2.5. Datenverletzungen .....	16
2.6. Bußgelder .....	16
2.7. Vorbereitung für die Einhaltung des DSGVO .....	17
2.8. Bewusstsein der DSGVO – ein Jahr nach Implementierung .....	20
<b>3. ePrivacy (Schutz der Privatsphäre in der elektronischen     Kommunikation) .....</b>	<b>23</b>
3.1. Kernpunkte des Vorschlags der Europäischen Kommission .....	24
3.2. Strengere Datenschutzbestimmungen für die elektronische Kommunikation .....	26
3.3. Anwendbares Recht und grenzüberschreitende Situationen .....	27
3.4. Zusammenhang zwischen DSGVO & ePR .....	27
3.5. Vorteile für Bürger und Unternehmen .....	28
<b>4. Schutz personenbezogener Daten .....</b>	<b>29</b>
4.1. Welche Regelungen ergänzen die europäischen Regelungen .....	30
4.1.1. Österreich .....	30
4.1.2. Tschechien .....	30
4.1.3. Portugal .....	32
4.1.4. Spanien .....	34
<b>5. Nich-personenbezogene Daten .....</b>	<b>39</b>

5.1. Freier Datenverkehr innerhalb der EU.....	40
5.2. Übertragung von Daten.....	41
5.3. Verfahren für die Zusammenarbeit zwischen Behörden.....	42
5.4. Datenverfügbarkeit für zuständige Behörden .....	42
5.5. Strafen für Verstöße.....	42
<b>6. Systematisierter Inhaltskatalog.....</b>	<b>44</b>
<b>7. Schlussfolgerung .....</b>	<b>46</b>
<b>8. Quellen.....</b>	<b>47</b>



## Liste der Abkürzungen

**DPA:** Datenschutzbehörde (Data Protection Authority)

**DSB:** Datenschutzbeauftragter

**DSG:** Österreichisches Datenschutzgesetz

**DSGVO:** Deutsche Datenschutz-Grundverordnung

**EEA:** Europäischer Wirtschaftsraum (European Economic Area)

**ePR:** ePrivacy Regulation (ePrivacy Verordnung - Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation)

**EU:** Europäische Union (European Union)

**DSGVO:** General Data Protection Regulation (Datenschutz- Grundverordnung – DSGVO)

## Abbildungen

Abbildung 1 - DSGVO .....	7
Abbildung 2 – Prinzipien der DSGVO .....	9
Abbildung 3 – Verarbeitung personenbezogener Daten.....	10
Abbildung 4 – Datenverantwortlicher und Datenverarbeiter .....	11
Abbildung 5 – Verarbeitung personenbezogener Daten .....	13
Abbildung 6 – Beispiel für die Zustimmung .....	14
Abbildung 7 – Rechte nach DSGVO .....	15
Abbildung 8 - DSGVO Konformität.....	18
Abbildung 9 - ePrivacy Regeln.....	25
Abbildung 10 – Schutz der Privatsphäre online.....	27
Abbildung 11 - DSGVO vs ePR .....	28
Abbildung 12 – Vorteile für Bürger und Unternehmen .....	28
Abbildung 13 – Nicht-personenbezogene Daten .....	39

## Tabellen

Tabelle 1 - Gesetzgebung zum Schutz personenbezogener Daten .....	36
---	----

# 1. Einführung

Heutzutage ist die Welt zunehmend abhängig von Daten, da Daten für zahlreiche Wirtschaftsakteure einen erheblichen Mehrwert darstellen können. In der Europäischen Union (EU) gibt es Regelungen bezüglich der personenbezogenen Daten: Die Verordnung (EU) 2016/679 (Allgemeine Datenschutzverordnung) und die Verordnung über den Schutz der Privatsphäre in der elektronischen Kommunikation (ePR), die ein Vorschlag für die Datenschutzrichtlinie für elektronische Kommunikation von 2002 (Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG) ist.

Die Verordnung (EU) 2018/1807 zielt darauf ab, Hindernisse für den freien Verkehr nicht-personenbezogenen Daten zwischen den EU-Mitgliedsstaaten und die Informationstechnologie in Europa zu beseitigen. Zusammen mit der Allgemeinen Datenschutzverordnung (DSGVO) gewährleistet diese Verordnung einen umfassenden und kohärenten Ansatz für den freien Verkehr aller Daten in Europa. Der Anwendungsbereich der ePR soll das Vertrauen und die Sicherheit im digitalen Binnenmarkt durch die Aktualisierung des Rechtsrahmens für die ePrivacy (ePR) stärken.

Diese drei Verordnungen gelten für jedes europäische Land, auch wenn es einige Öffnungsklauseln gibt, die den nationalen Gesetzgebern einen gewissen Spielraum lassen.

In diesem Bericht finden Sie die wichtigsten Informationen im Zusammenhang mit diesen Rechtsvorschriften. Darüber hinaus wird in diesem Dokument erörtert, wie die europäische Gesetzgebung zum Schutz personenbezogener Daten in Österreich, Spanien, Portugal und der Tschechischen Republik angepasst wurde.



## 2. DSGVO

Die DSGVO (Verordnung (EU) 2016/679) ist ein EU-Gesetz über den Datenschutz und die Privatsphäre für alle einzelnen Bürger der EU und des Europäischen Wirtschaftsraums (EWR). Sie regelt auch den Export personenbezogener Daten außerhalb der oben genannten geografischen Gebiete. Die DSGVO ist seit Mai 2018 in Kraft und hat drei Hauptziele:

- a) **Harmonisierung der Datenschutzgesetze** in ganz Europa;
- b) **Schutz und Stärkung des Datenschutzes aller EU-Bürger;**
- c) **Neugestaltung der Art und Weise, wie Organisationen in der gesamten Region an den Datenschutz herangehen.**

Abbildung 1 - DSGVO



Quelle: Business2Community (2019)

Mit der DSGVO signalisiert Europa seine feste Haltung zum Datenschutz und zur Datensicherheit, und die DSGVO gestaltet die Art und Weise, wie Unternehmen/Organisationen Daten verwalten, neu. Die DSGVO wird angewandt bei:

- a) **einem Unternehmen oder eine Einrichtung, die personenbezogene Daten im Rahmen der Aktivitäten einer ihrer in der EU niedergelassenen Zweigstellen verarbeitet**, unabhängig davon, wo die Daten verarbeitet werden; oder
- b) **einem Unternehmen oder eine Einrichtung mit Sitz außerhalb der EU, das Waren/Dienstleistungen** (gegen Bezahlung oder kostenlos) anbietet oder das Verhalten von Einzelpersonen in der EU überwacht.

## 2.1. Prinzipien der DSGVO

Die DSGVO hat einige allgemeine Grundsätze bezüglich der Verarbeitung von personenbezogenen Daten. Einer dieser Grundsätze verlangt, dass die Daten transparent verarbeitet werden, was bedeutet, dass dieser Prozess klar und legitim sein muss. Auch muss die Menge der verarbeiteten Daten auf ein Minimum beschränkt werden, je nach Zweck müssen die Daten korrekt sein und die Aufbewahrungszeit muss auf einen an den Zweck gebundenen Zeitraum beschränkt werden. Zusätzlich müssen die Integrität und die Vertraulichkeit der Daten geschützt werden. Die wichtigsten Grundsätze der DSGVO sind in der nächsten Abbildung dargestellt.



**Abbildung 2 – Prinzipien der DSGVO**



**Quelle:** I-scoop (2019)

Im Allgemeinen ist die Hauptanlaufstelle für Fragen zum Datenschutz das Datenschutzgesetz (Data Protection Act, DPA) in jenem EU-Mitgliedsstaat, in dem Ihr Unternehmen/Organisation ansässig ist. Wenn Ihre Firma/Organisation jedoch Daten in verschiedenen EU-Mitgliedsstaaten verarbeitet oder Teil einer Gruppe von Unternehmen ist, die in verschiedenen EU-Mitgliedsstaaten ansässig sind, kann die Hauptanlaufstelle eine Datenschutzbehörde in einem anderen EU-Mitgliedsstaat sein.

Finden Sie Ihre nationale Datenschutzbehörde unter:

[https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en)

## **2.2. Verwendung, Verarbeitung, Speicherung und Übertragung von Daten in der EU**

Als Einzelperson, Unternehmen oder Organisation haben Sie das Recht, personenbezogenen Daten zu nutzen, zu sammeln, zu speichern, zu übertragen oder zu verwalten und Rechenzentren oder Cloud-Dienste überall in der EU zu

nutzen. Die Regeln für den Umgang mit personenbezogenen Daten unterscheiden sich von den Regeln für die nicht-personenbezogenen Daten. Dennoch werden personenbezogene und nicht-personenbezogene Daten oft zusammen gesammelt und gespeichert, und dies wird als gemischte Daten bezeichnet. Es gibt einige Themen, die die Unternehmen/Organisationen bei der Verarbeitung der in der nächsten Abbildung dargestellten personenbezogenen Daten erfüllen müssen.

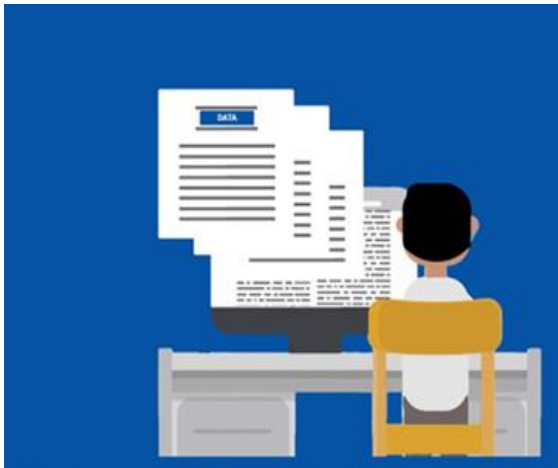
**Abbildung 3 – Verarbeitung personenbezogener Daten**



**Quelle:** European Commission (2019)

Während der Verarbeitung können personenbezogene Daten verschiedene Unternehmen oder Organisationen durchlaufen, und innerhalb dieses Zyklus gibt es zwei Hauptprofile, die sich mit der Verarbeitung personenbezogener Daten befassen: den Datenverantwortlichen und den Datenverarbeiter.

**Abbildung 4 – Datenverantwortlicher und Datenverarbeiter**



**Datenverantwortlicher:**

entscheidet über den Zweck und die Art und Weise, in der die personenbezogenen Daten verarbeitet werden

**Datenverarbeiter:**

hält und verarbeitet Daten im Auftrag des Datenverantwortlichen

**Quelle:** Eigene Ausarbeitung

Unternehmen/Organisationen, die Daten verarbeiten, sind verpflichtet, Aufzeichnungen über die Verarbeitungsaktivitäten zu führen, es sei denn, sie haben weniger als 250 Mitarbeiter. Außerdem müssen Unternehmen/Organisationen einen Datenschutzbeauftragten (DSB) benennen, wenn einer der folgenden Aspekte zutrifft:

- Wenn die Verarbeitung durch eine öffentliche Einrichtung (mit Ausnahme von Gerichten) durchgeführt wird;
- Wenn die Kerntätigkeiten des Verarbeiters "aus Verarbeitungsvorgängen bestehen, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Maßstab erfordern";
- wenn besondere Datenkategorien oder "Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten" verarbeitet werden.

Der Datenschutzbeauftragte (DSB) ist jemand, der möglicherweise vom Unternehmen benannt wurde und dafür verantwortlich ist, zu überwachen, wie personenbezogene Daten verarbeitet werden, und die Mitarbeiter, die personenbezogene Daten verarbeiten, über ihre Verpflichtungen zu informieren und zu beraten. Der DSB kann ein Mitarbeiter Ihrer Organisation sein oder auf der Grundlage eines Dienstkontakts extern beauftragt werden. Der DSB arbeitet auch mit der Datenschutzbehörde (DPA) zusammen, und fungiert als Kontaktstelle gegenüber der DPA und den Bürgern.

### **2.3. Zustimmung zur Datenverarbeitung**

Die Verantwortung für die Einhaltung der DSGVO hängt von Unternehmen/Organisationen ab, die personenbezogene Daten verarbeiten. Unter Berücksichtigung der Art, des Umfangs, des Kontextes und der Zwecke der Verarbeitung sowie der Strenge für die Rechte und Freiheiten der Bürger hat der für die Verarbeitung der Daten Verantwortliche geeignete technische und organisatorische Maßnahmen durchzuführen, um sicherzustellen und nachweisen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Verordnung erfolgt. Diese Maßnahmen sind zu überprüfen und erforderlichenfalls zu aktualisieren. Beispiele für diese Maßnahmen sind Pseudonymisierung oder Verschlüsselung.

Die DSGVO wendet strenge Regeln für die Verarbeitung von Daten auf der Grundlage der Einwilligung an. Der Zweck dieser Regeln besteht darin sicherzustellen, dass der Einzelne versteht, in was er/sie einwilligt. Das bedeutet, dass die Einwilligung frei durch eine bestätigende Handlung gegeben werden sollte, z.B. durch das Ankreuzen eines Kästchens im Internet oder durch die Unterzeichnung eines Formulars. Wenn jemand in die Verarbeitung seiner personenbezogenen Daten einwilligt, können die Daten nur für die Zwecke verarbeitet werden, für die die Einwilligung erteilt wurde. Wichtig ist auch, dass Sie die Personen eindeutig darüber informieren müssen, wer die personenbezogenen Daten über sie verarbeitet und aus welchen Gründen. Zum

Beispiel sollte mindestens die Details folgender Abbildung enthalten sein:

**Abbildung 5 – Verarbeitung personenbezogener Daten**



**Quelle:** European Commission (2019)

In einigen Situationen müssen die von Ihnen bereitgestellten Informationen auch angegeben werden:

- Die Kontaktinformationen des DSB (falls zutreffend);
- Welches ist das legitime Interesse, das das Unternehmen verfolgt, wenn Sie sich auf diesen Rechtsgrund für die Verarbeitung berufen;
- Die Maßnahmen, die für die Übermittlung der Daten in ein Land außerhalb der EU angewandt werden;
- Wie lange die Daten gespeichert werden;
- Die Datenschutzrechte des Einzelnen;
- Wie die Einwilligung zurückgezogen werden kann (wenn die Einwilligung der rechtliche Grund für die Verarbeitung ist);
- Ob eine gesetzliche oder vertragliche Verpflichtung zur Bereitstellung der Daten besteht;
- Im Falle einer automatisierten Entscheidungsfindung Informationen über die Logik, die Bedeutung und die Folgen der Entscheidung.

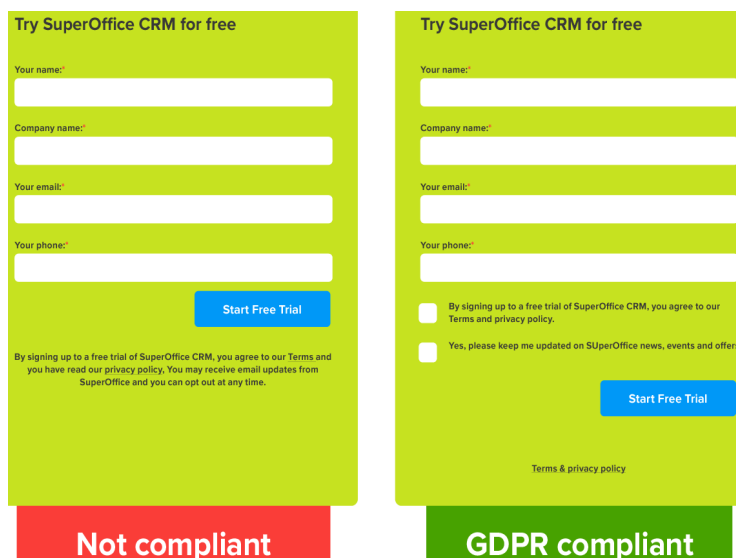
Es ist wichtig zu beachten, dass diese Informationen klar sein sollten und dass Sie

eine einfache/klare Sprache verwenden müssen.

Die Bedingungen für die Zustimmung wurden verschärft, und Unternehmen/Organisationen sind nicht mehr in der Lage, lange unleserliche und mit juristischen Begriffen und Konzepten vollgepackte Bedingungen zu verwenden. Der Antrag auf Zustimmung muss in einer verständlichen und leicht zugänglichen Form gestellt werden, wobei der Zweck der Datenverarbeitung an diese Zustimmung geknüpft werden muss. Die Einwilligung muss klar und deutlich von anderen Angelegenheiten unterscheidbar sein und in einer verständlichen und leicht zugänglichen Form und Sprache erteilt werden.

Die nächste Abbildung zeigt ein Beispiel dafür, was getan werden sollte. In der nächsten Abbildung können Sie sehen, dass die DSGVO für Unternehmen/Organisationen eine Menge Dinge verändert hat. Daher müssen Unternehmen ihre Geschäftsprozesse, Anträge und Formulare überprüfen, um beispielsweise mit dem E-Mail-Marketing konform zu sein. Um sich für die Kommunikation anzumelden, müssen Interessenten ein Formular ausfüllen oder ein Kästchen ankreuzen und dann in einer weiteren E-Mail bestätigen, dass es sich um ihre Aktionen handelt.

**Abbildung 6 – Beispiel für die Zustimmung**



Quelle: SuperOffice (2019)

## 2.4. Recht auf Zugang und Recht auf Datenübertragbarkeit

Unternehmen und Organisationen müssen sicherstellen, dass Einzelpersonen das Recht haben, kostenlos auf ihre personenbezogenen Daten zuzugreifen. Wenn Sie eine solche Anfrage erhalten, müssen Sie dies tun:

- Geben Sie ihnen die Information, ob Sie ihre personenbezogenen Daten verarbeiten;
- Informieren Sie sie über die Verarbeitung (Zweck der Verarbeitung, betroffene Kategorien personenbezogener Daten usw.);
- Lassen Sie ihnen eine Kopie der verarbeiteten personenbezogenen Daten (in einem zugänglichen Format) zukommen.

Mit der neuen DSGVO wird es immer wichtiger, den Kunden oder die Person, deren Daten Sie verarbeiten, darüber zu informieren, was mit ihren Daten geschieht. Die Rechte, die Sie kennen müssen, sind in der folgenden Abbildung zusammengefasst.

Abbildung 7 – Rechte nach DSGVO



Quelle: Serveit (2019)



Diese Rechte werden dem Einzelnen gewährt, um sein Privatleben zu schützen und die digitalen Fußabdrücke zu kontrollieren, die er bei der Nutzung internetbasierter Anwendungen und Dienste hinterlässt. Diese Rechte sollen Offenheit, Kontrolle und Vertrauen zwischen allen Beteiligten schaffen.

## **2.5. Datenverletzungen**

Eine Datenverletzung liegt vor, wenn die personenbezogenen Daten entweder versehentlich oder unrechtmäßig an unberechtigte Empfänger weitergegeben, vorübergehend nicht verfügbar gemacht oder geändert werden.

Wenn es zu einer Datenverletzung kommt und die Verletzung eine Gefahr für die Rechte und Freiheiten des Einzelnen darstellt, sollten Sie Ihre Datenschutzbehörde innerhalb von 72 Stunden, nachdem Sie von der Verletzung erfahren haben, benachrichtigen.

## **2.6. Bußgelder**

Die Bußgelder werden immer höher und die Fristen werden immer kürzer. Nach der DSGVO sind nun alle Mitglieder verpflichtet, Verletzungen der Datensicherheit zu melden, wenn eine Datenverletzung wahrscheinlich "eine Gefahr für die Rechte und Freiheiten des Einzelnen darstellt". Dies muss innerhalb von 72 Stunden nach Bekanntwerden der Verletzung erfolgen. Datenverarbeiter müssen auch ihre Kunden, die für die Verarbeitung Verantwortlichen, unverzüglich nach dem ersten Bekanntwerden einer Datenverletzung benachrichtigen.

Daher führt die DSGVO eine strengere Durchsetzungsregelung ein und setzt die Unternehmen einer erhöhten finanziellen Haftung aus. Es sind mehrere hochrangige Fälle im Gange, die bei schweren Verstößen zu Geldstrafen von bis zu 4% des Jahresbetrags eines Unternehmens führen können. Die Höchststrafe beträgt 20 Millionen Euro oder 4% der weltweiten Einnahmen, je nachdem, welcher Betrag höher ist. Die Datenschutzbehörden können auch Sanktionen wie Verbote der Datenverarbeitung oder öffentliche Verweise aussprechen.

Gemäß DSGVO werden die Geldstrafen von der Datenschutzbehörde in jedem EU-

Land verwaltet. Die endgültige Höhe der Geldbußen wird bewertet nach: Schwere und Art; Absicht; Milderung; Vorsichtsmaßnahmen; Vorgeschichte; Zusammenarbeit; Datenkategorie; Meldung; Zertifizierung; erschwerende/mildernde Faktoren. Wenn die Aufsichtsbehörden feststellen, dass eine Organisation mehrere DSGVO-Verstöße aufweist, wird sie nur für den schwersten Fall bestraft, vorausgesetzt, dass alle Verstöße Teil desselben Verarbeitungsvorgangs sind.

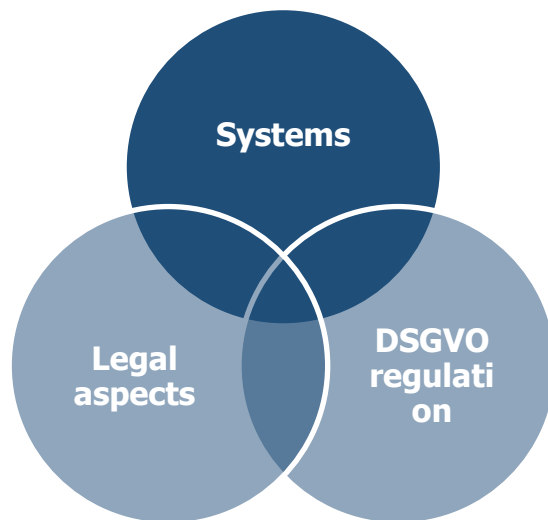
## 2.7. Vorbereitung für die Einhaltung des DSGVO

Die Anwendung von DSGVO stellt strenge Anforderungen an die Art und Weise, wie Unternehmen/Organisationen personenbezogene Daten sammeln, speichern und verwalten. Angesichts dieses Hintergrunds bietet die DSGVO den Bürgern der EU eine größere Kontrolle über ihre personenbezogenen Daten und stellt sicher, dass ihre Informationen in ganz Europa sicher geschützt werden, unabhängig davon, ob die Datenverarbeitung in der EU stattfindet oder nicht.

DSGVO umfasst drei Hauptbereiche, die jedes Unternehmen berücksichtigen muss (siehe Abbildung 5):

1. The **DSGVO- Verordnung** selbst;
2. Die **Systeme**, die Sie zur Speicherung aller Ihrer Kundendaten verwenden;
3. Die **rechtlichen Aspekte** der Verordnung und wie sie sich auf die Art und Weise auswirkt, wie Sie mit personenbezogenen Daten umgehen.

**Abbildung 8 - DSGVO Konformität**



Quelle: eigene Ausarbeitung

Darüber hinaus ist ein wesentlicher Bestandteil der DSGVO-Gesetzgebung "Privacy by Design" (Datenschutz durch Technikgestaltung). Privacy by Design erfordert, dass alle Abteilungen in einem Unternehmen/einer Organisation ihre Daten und den Umgang mit ihnen genau unter die Lupe nehmen. Es gibt viele Themen, die ein Unternehmen betreffen, um DSGVO-konform zu sein. Hier finden Sie einige Schritte, die Ihnen helfen können, diesen Prozess in Gang zu bringen.

- 1. Zeichnen Sie die Daten Ihres Unternehmens auf:** Stellen Sie fest, woher alle personenbezogenen Daten in Ihrem gesamten Unternehmen stammen, und dokumentieren Sie, was Sie mit den Daten tun. Stellen Sie fest, wo sich die Daten befinden, wer auf sie zugreifen kann und ob mit den Daten, die Sie haben, Risiken verbunden sind.
- 2. Bestimmen Sie, welche Daten Sie aufbewahren müssen:** DSGVO ermutigt zu einem disziplinierteren Umgang mit personenbezogenen Daten. Aus diesem Grund ist es entscheidend, nur die Informationen aufzubewahren, die notwendig sind, und alle Daten, die Sie nicht verwenden, zu entfernen. Wenn Ihre Firma/Organisation eine Menge Daten ohne wirklichen Nutzen gesammelt hat, ist

es an der Zeit, zu überlegen, welche Daten für Ihre Firma/Organisation wichtig sind. Bei der Bereinigung können Sie diesen Fragen folgen:

- Warum genau archivieren wir diese Daten, anstatt sie einfach zu löschen?
- Warum speichern wir all diese Daten?
- Was versuchen wir zu erreichen, indem wir all diese Kategorien von personenbezogenen Daten sammeln?  
Ist der finanzielle Gewinn, diese Informationen zu löschen, größer als sie zu verschlüsseln?

**3. Setzen Sie Sicherheitsmaßnahmen ein:** Entwickeln und implementieren Sie Schutzmaßnahmen in Ihrer gesamten Infrastruktur, um Datenverletzungen einzudämmen. Dies bedeutet, Maßnahmen gegen Datenverstöße zu ergreifen, um im Falle eines Verstoßes schnell handeln zu können und Personen und Behörden zu benachrichtigen.

**4. Überprüfen Sie Ihre Dokumentation:** Nach DSGVO müssen Einzelpersonen der Erfassung und Verarbeitung ihrer Daten ausdrücklich zustimmen. Vorab angekreuzte Kästchen und die implizite Einwilligung werden nicht mehr akzeptiert.

## 2.8. Bewusstsein der DSGVO – ein Jahr nach Implementierung

Ein Jahr nach Implementierung der DSGVO, der wichtigsten und bedeutendsten Änderung des Rechtsrahmens für den Datenschutz, werden sich die europäischen Bürgerinnen und Bürger der Rechte und Pflichten, die sich aus der Anwendung der Gesetzgebung zum Schutz personenbezogener Daten ergeben, immer mehr bewusst.

Die im Juni 2019 veröffentlichten Ergebnisse des von der Europäischen Kommission durchgeführten Berichts zum Thema "Allgemeine Datenschutzverordnung" ("General Data Protection Regulation") zeigen, dass die Mehrheit (mehr als zwei Drittel) der Europäer von der DSGVO und von den durch die DSGVO garantierten Rechten gehört haben, mit Ausnahme des Mitspracherechts bei automatisierten Entscheidungen (41%). Die Länder, die mehr über DSGVO wissen sind: Schweden (90%), die Niederlande (87%) und Polen (86%). Darüber hinaus haben die Befragten im Alter von 25-54 Jahren (75%) am ehesten von der DSGVO gehört, die Befragten im Alter von 15-54 Jahren sind sich ihrer Rechte auf personenbezogene Daten eher bewusst als die Befragten im Alter von 55 Jahren oder älter, und Männer sind sich im Vergleich zu Frauen eher über jedes dieser Rechte im Klaren. Je länger ein Befragter in der Ausbildung blieb, desto wahrscheinlicher ist es, dass er über diese Gesetzgebung Bescheid weiß.

Darüber hinaus haben Irland, die Slowakei und Polen einige der höchsten Anteile der Befragten, die von DSGVO gehört haben und wissen, was es ist, und auch die höchsten Anteile der Befragten, die von allen Rechten gehört haben, nach denen in der durchgeführten Umfrage gefragt wurde.

Was das Bewusstsein der für den Datenschutz zuständigen nationalen Behörden betrifft, so gibt die Mehrheit (6 von 10) an, dass sie von der Existenz einer öffentlichen Behörde in ihrem Land gehört haben, die für den Schutz ihrer Rechte in Bezug auf ihre personenbezogenen Daten verantwortlich ist.

Seit 2018 sind die nationalen Datenschutzbehörden für die Durchsetzung der neuen Vorschriften zuständig und koordinieren ihre Maßnahmen besser. Dennoch gibt es in Bezug auf die Fragen der Einhaltung noch einiges zu tun, da es sich um

einen dynamischen Prozess handelt.

Laut dem Deloitte Legal-Bericht "Die DSGVO: Sechs Monate nach der Umsetzung: Praktiker-Perspektiven" ("The DSGVO: Six months after implementation: Practitioner perspectives") gibt es noch einiges an Arbeit bezüglich der Umsetzung des DSGVO zu tun. Die wichtigsten Schlussfolgerungen dieses Berichts legen nahe, dass dies wichtig ist:

- Wenn es um die Einhaltung des DSGVO geht, muss man sich zunächst über die Einzelheiten der Verarbeitung personenbezogener Daten informieren, denn es fehlt noch das Bewusstsein für die Grundregeln;
- Verbesserung der Transparenz über die Verarbeitung personenbezogener Daten für die betroffenen Personen, wie in der DSGVO gefordert;
- Verbesserung der Leitlinien, Empfehlungen oder offiziellen Positionen der Datenschutzaufsicht des Landes;
- Durchführung von Schulungen zur Sensibilisierung hinsichtlich der relevantesten DSGVO-Anforderungen des gesamten Personals, da jeder verstehen muss, wie man dieses in seiner täglichen Arbeit anwenden und umsetzen kann;
- Die Einführung von Sicherheitsmaßnahmen, die über die geforderten Mindeststandards hinausgehen (zum Beispiel die Verschlüsselung aller an E-Mails angehängten Dokumente);
- Schaffen Sie eine nicht-kommerzielle Plattform zum Austausch von spezialisiertem Rechtswissen, guten Praktiken und praktischen und kreativen Lösungen unter Spezialisten für den Schutz personenbezogener Daten;
- Richtlinien für kleine und mittlere Unternehmen, um ihnen zu helfen, die neue gesetzliche Regelung zum Schutz personenbezogener Daten in der Praxis anzuwenden;
- Erstellung mehrerer Vorlagen zur Behandlung verschiedener Fragen im Zusammenhang mit der DSGVO (Erfassung, Umsetzung und Übertragung des Schutzes personenbezogener Daten und Beantragung der Genehmigung zur Übertragung personenbezogener Daten);

- Entwicklung einiger Initiativen, die frühzeitig auf Schulen und Ausbildungsmaterialien abzielen.



### 3. ePrivacy (Schutz der Privatsphäre in der elektronischen Kommunikation)

Die Strategie für den digitalen Binnenmarkt zielt darauf ab, das Vertrauen und die Sicherheit der digitalen Dienste zu erhöhen. Die Reform des Datenschutzrahmens, insbesondere die Übernahme der DSGVO, war eine Schlüsselmaßnahme dazu. Die Strategie für den digitalen Binnenmarkt kündigte auch die Überprüfung der Richtlinie 2002/58/EG (die Datenschutzrichtlinie für elektronische Kommunikation) an, um ein hohes Maß an Datenschutz für die Nutzer elektronischer Kommunikationsdienste zu gewährleisten.

Die ePrivacy-Richtlinie für elektronische Kommunikation legt einige Regeln fest, die den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation gewährleisten soll. Zur elektronischen Kommunikation gehören unter anderem E-Mail Anwendungen, Telefon, Instant Messaging, Spam, Direktmarketing, Telekommunikationsunternehmen, Entwickler von mobilen Anwendungen und Online-Werbenetzwerke. Diese Richtlinie bietet auch Schutz für Nutzer und Abonnenten elektronischer Kommunikationsdienste vor unerbetenen Nachrichten. Die ePrivacy-Richtlinie für elektronische Kommunikation verlangt von Anbietern elektronischer Kommunikationsdienste wie Internetzugang, Festnetz- und Mobiltelefonie:

- a) geeignete Maßnahmen zu ergreifen, die die Sicherheit der elektronischen Kommunikationsdienste gewährleisten;
- b) die Vertraulichkeit der Kommunikation und der damit verbundenen Verkehrsdaten in öffentlichen Netzen zu gewährleisten.

Die **drei Hauptziele der ePrivacy- Richtlinie** sind Folgende:

- Gewährleistung eines gleichwertigen Schutzes des Grundrechts auf Privatsphäre und Vertraulichkeit bei der Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation in der gesamten EU. Dieser Schutz wird auch

Teilnehmern gewährt, die juristische Personen sind;

- Gewährleistung eines gleichwertigen Schutzniveaus in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation, um das Grundrecht auf Datenschutz zu schützen;
- Gewährleistung freien Datenverkehrs von personenbezogenen Daten, die im Bereich der elektronischen Kommunikation verarbeitet werden, sowie des freien Datenverkehrs von elektronischen Kommunikationsendgeräten und -diensten in der EU.

Die ePR wird die bestehende EU-Datenschutzrichtlinie für elektronische Kommunikation und die Richtlinie für elektronische Kommunikation von 2002 ersetzen. Diese Regelung ist wichtig, weil sie bedeutet, dass sie ein Rechtsakt ist und in ihrer Gesamtheit in allen Mitgliedsstaaten wie die DSGVO durchsetzbar sein wird. Darüber hinaus muss dieser Vorschlag die Übereinstimmung mit der DSGVO gewährleisten.

Während die DSGVO den Schutz personenbezogener Daten gewährleistet, zielt die ePR darauf ab, die Vertraulichkeit der Kommunikation zu gewährleisten, die auch nicht-personenbezogene Daten und Daten in Bezug auf eine juristische Person enthalten kann.

Die ePR sollte am 25. Mai 2018 zusammen mit der DSGVO in Kraft treten, doch die fortgesetzten Beratungen und die Lobbyarbeit einiger haben die Anwendung dieser Verordnung verzögert.

### **3.1. Kernpunkte des Vorschlags der Europäischen Kommission**

Der Vorschlag für eine Verordnung über ein hohes Maß an Datenschutzvorschriften für die gesamte elektronische Kommunikation beinhaltet:

## Abbildung 9 - ePrivacy Regeln

**Communications content and metada:** privacy is guaranteed for communications content and metada for example, time of a call and location. Metadata have a high privacy component and is to be anonymised or deleted if users did not give their consent, unless the data is needed for billing.

**New players:** Privacy rules will in the future also apply to new players providing eletronic communications services such as WhatsApp, Facebook Messenger ans Skype. This will ensure that these services guarantee the same level of confidentiality of communications as traditional telecoms operators.

**Stronger rules:** All people and businesses in the EU will enjoy the same level of protection of their eletronic communications through this directly applicable regulation. Businesses will also benefit from one single set of rules across the EU.

**New business opportunities:** once consent is given for communications data - content and/or metadata - to be processed, traditional telecommunications operators will have more oportunties to provide additional services and to develop their businesses.

**Simples rules on cookies:** the cookie provision, which has resulted in an overload of consent requests for internet users, will be stramlined. The new rule will be more user-friendly as browser setting and other identifiers. The proposal also clarifies that no consent is needed for non-privacy instrusive cookies improving internet experience or cookies used by a website to count the number of visitors.

**Protection agains spam:** this proposal bans unsolicited eletronic communications by emails, SMS and automated calling machines. Depending on national law people will either be protected by default or be able to use a do-not-call list to not receive marketing phone calls. Marketing callers will need to display their phone number or use a special pre-fix that indicates a marketing call.

**More effective enforcement:** the enforcement of the confidentiality rules in the regulation will be the responsibility of data protection authorities, already in charge of the rules under the GDPR.

**Quelle:** European Commission (2019)

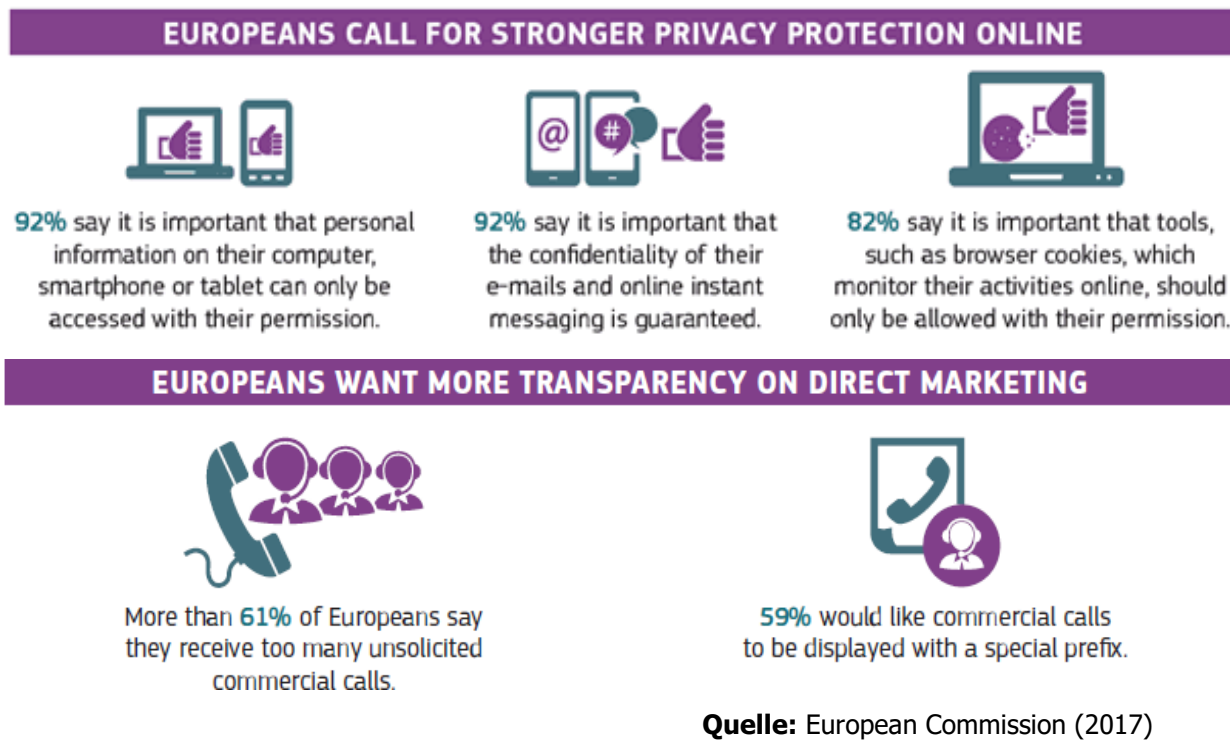
### **3.2. Strengere Datenschutzbestimmungen für die elektronische Kommunikation**

Wie wir bereits gesehen haben, nutzen immer mehr Europäer Online-Kommunikationsdienste, und mit der ePR ist die elektronische Kommunikation der Europäer unabhängig von der verwendeten Technologie vertraulich, die vorgeschlagenen Regeln werden auch für internetbasierte Sprach- und Internet-Messaging-Dienste gelten.

In der nächsten Abbildung können wir sehen, dass die Europäer einen stärkeren Schutz der Privatsphäre online benötigen, insbesondere auf ihren mobilen Geräten (Computer, Smartphone oder Tablet).

Darüber hinaus wollen die Europäer mehr Transparenz beim Direktmarketing. Deshalb muss man bei dieser Regelung zustimmen, bevor Marketingbotschaften an sie durch automatische Anrufmaschinen, SMS oder E-Mail gerichtet werden. Sie müssen auch dem Empfang von Marketinganrufen zustimmen, es sei denn, das nationale Recht gibt ihnen das Recht, dem Empfang solcher Anrufe zu widersprechen. Zusätzlich müssen Marketing-Anrufer ihre Telefonnummer anzeigen oder eine spezielle Vorwahl verwenden, die auf einen Marketing-Anruf hinweist.

**Abbildung 10 – Schutz der Privatsphäre online**











### 3.3. Anwendbares Recht und grenzüberschreitende Situationen

Die ePrivacy-Richtlinie für elektronische Kommunikation enthält keine ausdrückliche Bestimmung hinsichtlich des anwendbaren nationalen Rechts. Dies kann zu Rechtsunsicherheit darüber führen, welches Recht in einem grenzüberschreitenden Kontext anzuwenden ist. Die unklare Situation ergibt sich aus dem Fehlen einer spezifischen Regelung des anwendbaren Rechts, was eine wirksame Anwendung der Regeln in einer grenzüberschreitenden Situation behindert.

### 3.4. Zusammenhang zwischen DSGVO & ePR

Es gibt nur wenige Unterschiede und Ähnlichkeiten bezüglich der DSGVO und der ePR. Während die ePR die Vertraulichkeit der elektronischen Kommunikation schützt, schützt die DSGVO personenbezogene Daten. Dies bedeutet, dass die ePR die DSGVO im Bereich der elektronischen Kommunikation ergänzt. In der nächsten Abbildung ist ein Vergleich zwischen DSGVO und ePR dargestellt.

**Abbildung 11 - DSGVO vs ePR**

General Data Protection Regulation	Proposal for the ePrivacy Regulation
<p>1. Covers <b>all personal data</b> independently on the means of transmission. </p>	<p>1. Covers electronic communications and the <b>integrity of the information</b> on one's device, independently whether it is personal or non-personal data. </p>
<p>2. Defines the right to personal data protection. </p>	<p>2. Right to the privacy and confidentiality of communications. </p>
<p>3. Introduces new rights for citizens and obligations for companies. </p>	<p>3. Ensures that mobile apps or internet services through which you communicate cannot intercept, record, listen into, or tap in your communications. </p>
<p>4. Starts to apply on 25 May 2018. </p>	<p>4. Proposed on 10 January 2017 and currently in the legislative process in the European Parliament and the Council. </p>


**Quelle:** European Commission (2016)

### 3.5. Vorteile für Bürger und Unternehmen


Nach Ansicht der Europäischen Kommission hat diese Verordnung einige Vorteile für Bürger und Unternehmen. Die wichtigsten Vorteile für Bürger und Unternehmen sind in der nächsten Abbildung zu sehen.

**Abbildung 12 – Vorteile für Bürger und Unternehmen**


BENEFITS FOR CITIZENS AND BUSINESSES




Cookies and tracking for online advertisement remain lawful, but will be governed by clearer rules giving choices to users from the outset when setting their settings.



Traditional telecommunications services will have new opportunities to process metadata to provide additional services and to develop their businesses.



By replacing the current ePrivacy Directive by a directly applicable Regulation, citizens and businesses benefit from one single set of rules instead of 28 different ones. This creates more legal certainty and reinforces trust in the internal market.



ePrivacy rules will be enforced by independent supervisory authorities already competent to enforce the General Data Protection Regulation. This will ensure their uniform application across the EU.

**Quelle:** European Commission (2017)

## 4. Schutz personenbezogener Daten

Laut der Europäischen Kommission sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Mit anderen Worten, personenbezogene Daten sind alle Informationen, die zur Identifizierung einer Person verwendet werden können.

Der EU-Rahmen für den Schutz der Privatsphäre und des Datenschutzes hat zwei Hauptverordnungen: DSGVO und ePR.

Die DSGVO 2016/679 ist eine EU-Verordnung über den Datenschutz und den Schutz der Privatsphäre für alle Bürger der EU und auch des EWR.

Die DSGVO ist am 25. Mai 2018 in jedem europäischen Land in Kraft getreten. Der Zweck des DSGVO ist es, allen EU-Mitgliedern ein einheitliches Datenschutzgesetz aufzuerlegen, so dass nicht mehr jeder Mitgliedsstaat seine eigenen Datenschutzgesetze schreiben muss und die Gesetze folglich in der gesamten EU einheitlich sind. Die Anforderungen des DSGVO zielen darauf ab, einen einheitlicheren Schutz von Verbraucher- und personenbezogene Daten in allen EU-Ländern zu schaffen.

Darüber hinaus konzentriert sich DSGVO darauf sicherzustellen, dass die Nutzer die über sie gesammelten Daten kennen, verstehen und ihnen zustimmen. Die DSGVO schützt personenbezogene Daten unabhängig von der Technologie (automatisierte oder manuelle Verarbeitung), die zur Verarbeitung dieser Daten nach vordefinierten Kriterien verwendet wird. Auch ist es egal, wie die Daten gespeichert werden (z.B. Video, Papier, etc...), in allen Fällen unterliegen die personenbezogenen Daten den Schutzanforderungen der DSGVO und der ePR.

Die ePR zielt darauf ab, ein hohes Maß an Schutz der Privatsphäre der Nutzer elektronischer Kommunikationsdienste zu gewährleisten. Sie wurde von der Europäischen Kommission im Januar 2017 als Teil ihrer Strategie für den digitalen Binnenmarkt vorgeschlagen und wird die Datenschutzrichtlinie für elektronische Kommunikation von 2002 ersetzen.

Obwohl die grundlegende Datenschutzverordnung als EU-Verordnung in jedem



EU-Mitgliedsstaat direkt anwendbar ist, enthält sie einige Öffnungsklauseln und lässt dem nationalen Gesetzgeber einen gewissen Spielraum, wie wir im folgenden Abschnitt sehen werden.

## 4.1. Welche Regelungen ergänzen die europäischen Regelungen

### 4.1.1. Österreich

Die angewandten Vorschriften zum Schutz personenbezogener Daten sind:

- **DSGVO - Datenschutz-Grundverordnung (DSVGO);**
- **ePR;**
- **Österreichisches Datenschutzgesetz (DSG)** das die DSGVO ergänzt;
- **Gesetz zur Anpassung des Datenschutzes 2018 und Gesetz zur Deregulierung des Datenschutzes 2018** (zwei Änderungen des Datenschutzgesetzes) wurden angenommen, um diese Öffnungsklauseln und Spielräume umzusetzen. Das Datenschutzanpassungsgesetz 2018 wurde im BGBl I Nr. 120/2017 veröffentlicht und das Datenschutzfreigabegesetz 2018 im BGBl I Nr. 24/2018 trat am 25. Mai 2018 in Kraft;
- **Datenschutzrichtlinie** ist eine Richtlinie für den Bereich Justiz und Inneres, die sich auf die EU-Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden für folgende Zwecke stützt: Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten, Vollstreckung von Strafen, freier Datenverkehr und Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (Österreichische Datenschutzbehörde, 2019).

### 4.1.2. Tschechien

Im Falle der Tschechischen Republik sind die folgenden Rechtsvorschriften

anwendbar:

- **DSGVO**;
- **ePR**;
- **Beschluss Nr. 205** (15. März 2010) befasst sich mit Fragen der Cybersicherheit und hat das Innenministerium der Tschechischen Republik als Koordinator für Fragen der Cybersicherheit und die nationale Behörde für dieses Gebiet eingerichtet;
- **Beschluss Nr. 380** (24. Mai 2010) der Interdepartementalen Koordinierungsrat für den Bereich der Cybersicherheit wurde eingerichtet;
- **Beschluss Nr. 564** (20. Juli 2011) steht im Zusammenhang mit der tschechischen Cybersicherheitsstrategie für den Zeitraum 2011-2015;
- **Beschluss Nr. 781** (19. Oktober 2011) richtete die Behörde als Koordinator für Angelegenheiten der Internetsicherheit sowie die nationale Behörde für den Bereich der Internetsicherheit ein;
- **Cybersicherheitsgesetz** (1. Jänner 2015) steht in direktem Zusammenhang mit Fragen der Cybersicherheit;
- **Anordnung Nr. 437/2017** (8. Dezember 2017) setzt die einschlägigen Rechtsvorschriften der EU um und regelt sektorale und Wirkungskriterien für die Bestimmung eines Betreibers einer wesentlichen Dienstleistung sowie Spezifikationen zur Bestimmung der Bedeutung der Auswirkungen einer Unterbrechung einer wesentlichen Dienstleistung auf die Sicherheit der sozialen und wirtschaftlichen Aktivitäten;
- **Verordnung Nr. 181/2014 Slg.** (19. Dezember 2014) über Cybersicherheit und die Änderung damit zusammenhängender Gesetze wurden in der Gesetzessammlung veröffentlicht: Verordnung Nr. 316/2014 Slg. über Sicherheitsmaßnahmen, Cybersicherheitsvorfälle und reaktive Maßnahmen ("Cybersicherheitsverordnung"); Verordnung Nr. 317/2014 Slg. über wichtige Informationssysteme und deren Bestimmungskriterien; und die Regierungsverordnung Nr. 315/2014 Slg. zur Änderung der Regierungsverordnung Nr. 315/2014 Slg. zur Änderung der Regierungsverordnung Nr. 432/2010 Slg. über

die Kriterien für die Identifizierung eines kritischen Infrastrukturelements;

- **Verordnung Nr. 82/2018 Slg.** (21. März 2018) steht im Zusammenhang mit Sicherheitsmaßnahmen, Cybersicherheitsvorfällen, reaktiven Maßnahmen, Anforderungen an die Berichterstattung über die Cybersicherheit und die Datenvernichtung (der Cybersicherheitserlass).

#### 4.1.3. Portugal

In Portugal ist der Rahmen für den Schutz personenbezogener Daten geregelt:

**DSGVO;**

- **ePR;**

- **ePrivacy Verordnung** (29. August 2012) die auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen, angewendet werden sollte, wobei die Bestimmungen des Gesetzes Nr. 67/98 vom 26. Oktober spezifiziert und ergänzt werden. Unternehmen, die öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, sollten interne Verfahren zur Beantwortung von Anfragen der zuständigen Justizbehörden nach Zugang zu den personenbezogenen Daten der Benutzer in Übereinstimmung mit den genannten Sondergesetzen einrichten. Gemäß dem Gesetz zum Schutz der Privatsphäre in der elektronischen Kommunikation unterliegt die Zustellung von unerbetenen Mitteilungen für die Direktwerbung der vorherigen Zustimmung des Teilnehmers, der eine Einzelperson oder der Benutzer ist;

- **Verfassung der Portugiesischen Republik (Artikel 35)** die festlegt, dass alle Bürger das Recht auf Zugang zu allen betreffenden computergestützten Daten über sie haben und das Recht haben, über die Verwendung, für die die Daten bestimmt sind, informiert zu werden. Daher sind sie nach diesem Gesetz berechtigt, die Berichtigung und Aktualisierung des Inhalts der Akten und Aufzeichnungen zu verlangen. Dieses Gesetz legt fest, was personenbezogene Daten sind, sowie die

Bedingungen für die automatische Verarbeitung, Verbindung, Übertragung und Nutzung und soll den Schutz durch eine unabhängige Verwaltungsbehörde gewährleisten;

- **Datenschutzverordnung - Gesetz 67/98** - (26. Oktober 1998) das den rechtlichen Rahmen bildet, der im Allgemeinen sowohl für den privaten als auch für den öffentlichen Sektor sowie für jede sektorale Tätigkeit gilt. Das Datenschutzgesetz zielt darauf ab, das Recht des Einzelnen auf Privatleben bei der Verarbeitung personenbezogener Daten zu schützen, indem es die Rechte und die damit verbundenen Verfahren natürlicher Personen (Betroffene) sowie die Rechte, Pflichten und die Haftung juristischer und natürlicher Personen bei der Verarbeitung personenbezogener Daten festlegt. Das Datenschutzgesetz legt auch Grundsätze und Pflichten fest, die die Datenbearbeiter bei der Verarbeitung personenbezogener Daten einhalten müssen. Der allgemeine Grundsatz dieses Gesetzes besagt, dass die Verarbeitung personenbezogener Daten transparent und unter strikter Beachtung der Privatsphäre und anderer Grundrechte, Freiheiten und Garantien erfolgen muss;

- **Gesetz 32/2008** (18. Juli 2008) in dem die Verpflichtungen zur Datenspeicherung festgelegt sind, die den Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste auferlegt werden. Dieses Gesetz bezieht sich auf die Vorratsspeicherung von Daten, die im Zusammenhang mit der Bereitstellung von öffentlich zugänglichen elektronischen Kommunikationsdiensten oder öffentlichen Kommunikationsnetzen erzeugt oder verarbeitet werden;

- **Electronic communication laws - Law 5/2014** - (10. Februar 2014) und das **ePrivacy Gesetz**. Gemäß diesen Gesetzen müssen diese Anbieter im Falle einer Sicherheits- oder Integritätsverletzung die Regulierungsbehörde (die Nationale Kommunikationsbehörde oder ANACOM), die "Comissão Nacional de Proteção de Dados" und unter bestimmten Umständen die Teilnehmer und Nutzer des Dienstes benachrichtigen;

- **EU- Richtlinie 2016/1148** betreffend Cybersicherheit. Im Rahmen dieser Richtlinie gibt es Maßnahmen für ein hohes gemeinsames Sicherheitsniveau von

Netz- und Informationssystemen in der gesamten EU ab Juli 2016. Diese Richtlinie ermöglicht die Ausweitung der Verpflichtung zur Durchführung von Sicherheitsmaßnahmen und zur Meldung von Sicherheitsverletzungen an andere Stellen.

#### 4.1.4. Spanien

In Spanien werden die folgenden Gesetze zum Schutz personenbezogener Daten angewandt:

- **DSGVO**;
- **ePR**;
- **Vertrag von Lissabon (die Charta der Grundrechte der EU) und die spanische Verfassung von 1978** die sich auf den Datenschutz und die Privatsphäre beziehen und beides Grundrechte sind;
- **Mehrere Verhaltenskodex für den Datenschutz**, die im Rahmen der früheren spanischen Datenschutzbestimmungen für verschiedene Sektoren genehmigt wurden;
- **Sektorspezifische Regelungen**, die auch Datenschutzbestimmungen enthalten, da bestimmte Kategorien personenbezogener Daten und bestimmte Verarbeitungsaktivitäten einen besonderen Schutz erfordern können, wie z.B. die Verarbeitung personenbezogener Daten in den Bereichen Finanzen, elektronische Kommunikation oder Gesundheit;
- **Neues spanisches Datenschutzgesetz** (25. Mai 2018 sieht in verschiedenen Bereichen spezifische Datenschutzbestimmungen vor, die nicht ausdrücklich in der DSGVO enthalten sind oder die zwar in der DSGVO enthalten sind, aber einen Umfang haben, der es den Mitgliedsstaaten erlaubt, detailliertere Regelungen einzuführen. Darüber hinaus enthält dieses Gesetz im spanischen Rechtssystem eine Liste von neuen Rechten der Bürger in Bezug auf neue Technologien, die als "digitale Rechte" bekannt sind. Dieses Gesetz beinhaltet auch eine Änderung des spanischen allgemeinen Wahlgesetzes, die es den politischen Parteien erlaubt, personenbezogene Daten für spezifische Wahlwerbemaßnahmen zu verarbeiten;

- **E-Commerce- Gesetz 34/2002 (LSSI)** und das **Allgemeines Telekommunikationsrecht 9/2014 (GTL)** die sich auf sektorspezifische Regelungen beziehen, können auch Datenschutzbestimmungen enthalten;
- **EU- Richtlinie 2016/680** (27. April 2016) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen und zum freien Datenverkehr sowie zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates;
- **Cybersicherheitscode** der alle aktualisierten Regeln zusammenfasst, die sich direkt auf die Cybersicherheit auswirken. Allerdings müssen die Cybersicherheitsvorschriften noch weiterentwickelt werden.

In der nächsten Tabelle finden Sie eine kurze Zusammenfassung der Gesetze zum Schutz personenbezogener Daten, die in Portugal, Tschechien, Portugal und Spanien angewendet werden.

**Tabelle 1 - Gesetzgebung zum Schutz personenbezogener Daten**

	Personenbezogene Daten		Nicht-personenbezogene Daten	Zusätzliche persönliche Datengesetzgebung	Kurze Erläuterung
	DSGVO	ePR	Regulation (EU 2018/1807)		
<b>Österreich</b>	✓	✓	✓	<b>Österreichisches Datenschutzgesetz</b>	Das Österreichische Datenschutzgesetz (DSG) ergänzt die DSGVO
				<b>Gesetz zur Anpassung des Datenschutzes 2018 (BGBl I Nr. 120/2017)</b>	Diese beiden Gesetze wurden verabschiedet, um die Öffnungsklauseln und Margen (zusätzlich zu den Änderungen zahlreicher materieller Gesetze) des Datenschutzgesetzes umzusetzen. Außerdem ergänzen diese Gesetze die DSGVO
				<b>Gesetz zur Deregulierung des Datenschutzes 2018 (BGBl I Nr. 24/2018)</b>	
				<b>Datenschutzrichtlinie</b>	Diese Richtlinie basiert auf der EU-Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung von Strafen, zum freien Datenverkehr.
<b>Tschechien</b>	✓	✓	✓	<b>Beschluss Nr. 205</b>	Behandlung von Fragen der Cybersicherheit und Einrichtung des Innenministeriums der Tschechischen Republik als Koordinator für Fragen der Cybersicherheit und der nationalen Behörde für dieses Gebiet
				<b>Beschlurr Nr. 380</b>	Einrichtung des Interdepartementalen Koordinierungsrat für den Bereich der Cybersicherheit
				<b>Beschluss Nr. 564</b>	Tschechische Cybersicherheitsstrategie 2011-2015



				<b>Beschluss Nr. 781</b>	Behörde als Koordinator für Cybersicherheitsangelegenheiten sowie national
				<b>Cybersicherheitsgesetz</b>	Dieses Gesetz regelt die Cybersicherheit in der Tschechischen Republik und ist seit dem 1. Januar 2015 in Kraft.
				<b>Andordnung Nr. 437/2017</b>	Dieser Erlass setzt die einschlägigen Rechtsvorschriften der EU um und regelt sektorale und Wirkungskriterien für die Bestimmung eines Betreibers einer wesentlichen Dienstleistung sowie Spezifikationen für die Bestimmung der Bedeutung der Auswirkungen der Unterbrechung einer wesentlichen Dienstleistung auf die Sicherheit der sozialen und wirtschaftlichen Aktivitäten.
				<b>Verordnung Nr. 181/2014 Slg.</b>	Im Zusammenhang mit der Cybersicherheit und der Änderung verwandter Verordnungen zu diesem Thema
				<b>Anordnung Nr. 82/2018 Slg.</b>	Im Zusammenhang mit Sicherheitsmaßnahmen, Cybersicherheitsvorfällen, reaktiven Maßnahmen, Anforderungen an die Berichterstattung über die Cybersicherheit und Datenvernichtung (der Cybersicherheitserlass)
<b>Portugal</b>	✓	✓	✓	<b>ePrivacy Verordnung</b>	Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen
				<b>Verfassung der Portugiesischen Republik (Artikel 35)</b>	Festlegung, dass alle Bürger das Recht auf Zugang zu allen sie betreffenden computergestützten Daten und das Recht haben, über die Verwendung, für die die Daten bestimmt sind, informiert zu werden, weshalb sie nach diesem Gesetz berechtigt sind, die Berichtigung und Aktualisierung des Inhalts der Akten und Aufzeichnungen zu verlangen. Dieses Gesetz legt fest, was personenbezogene Daten sind, sowie die Bedingungen für die automatische Verarbeitung, Verbindung, Übertragung und Nutzung und soll ihren Schutz durch eine unabhängige Verwaltungsbehörde gewährleisten
				<b>Gesetz 67/98 vom 26. Oktober</b>	Rechtsrahmen zum Datenschutzgesetz, der im Allgemeinen sowohl für den privaten als auch für

					den öffentlichen Sektor sowie für jede Tätigkeit im Sektor gilt
				<b>Gesetz 32/2008 vom 18. Juli</b>	Legt die Verpflichtungen zur Datenspeicherung fest, die den Anbietern von öffentlich zugänglichen elektronischen Kommunikationsdiensten auferlegt werden
				<b>Gesetz 5/2014 von 10. Februar and ePrivacy- Gesetz</b>	Nach diesen Gesetzen müssen diese Anbieter im Falle einer Sicherheits- oder Integritätsverletzung die Regulierungsbehörde (die Nationale Kommunikationsbehörde oder ANACOM), die "Comissão Nacional de Proteção de Dados" und, unter bestimmten Umständen, die Dienstteilnehmer und Nutzer benachrichtigen.
				<b>EU- Richtline 2016/1148</b>	Erlaubt die Ausdehnung der Verpflichtung zur Durchführung von Sicherheitsmaßnahmen und zur Meldung von Sicherheitsverletzungen auf andere Stellen
<b>Spanien</b>	✓	✓	✓	<b>Vertrag von Lissabon</b>	Sie beziehen sich auf den Datenschutz und die Privatsphäre und sind beides Grundrechte
				<b>Spanische Verfassung von 1978</b>	
				<b>Neues spanisches Datenschutzgesetz Gesetz 3/2018 vom 7. Dezember</b>	Spezifische Datenschutzbestimmungen in verschiedenen Bereichen vorzusehen, die nicht ausdrücklich in der DSGVO enthalten sind oder die in der DSGVO enthalten sind, jedoch mit einem Umfang, der die Einführung detaillierterer Vorschriften durch die Mitgliedstaaten ermöglicht
				<b>E-Commerce-Gesetz 34/2002 (LSSI)</b>	Bezogen auf sektorspezifische Regelungen
				<b>Allgemeines Telekommunikationsgesetz 9/2014 (GTL)</b>	
<b>EU-Richtline 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016</b>	Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen und zum freien Datenverkehr sowie zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates				
<b>Cybersecurity- Kodex</b>	nennt die wichtigsten zu berücksichtigenden Regeln für den Schutz des Cyberspace und zur Gewährleistung der oben genannten Cybersicherheit				

**Quelle:** Eigene Ausarbeitung des Autors

## 5. Nicht-personenbezogene Daten

Freier Fluss nicht-personenbezogene Daten bedeutet uneingeschränkte Bewegung von Daten über die Grenzen und Informationstechnologiesysteme in der EU.

Die Verordnung über den freien Verkehr nicht-personenbezogener Daten in der EU ist bereits in Kraft. Die genaue Bezeichnung für diese Verordnung ist die Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der EU.

Diese Verordnung zielt darauf ab, den freien Fluss von anderen als personenbezogenen Daten innerhalb der EU zu gewährleisten, indem sie Regeln bezüglich der Anforderungen an die Datenlokalisierung, die Verfügbarkeit von Daten für die zuständigen Behörden und die Portierung von Daten für professionelle Nutzer festlegt. Diese Verordnung gilt auch für die Verarbeitung anderer elektronischer Daten als personenbezogener Daten in der EU:

- Bereitstellung als Dienstleistung für Nutzer mit Wohnsitz oder Niederlassung in der Union, unabhängig davon, ob der Dienstanbieter in der Union niedergelassen ist oder nicht;
- Durchgeführt von einem Daten oder juristische Person mit Wohnsitz oder eine Niederlassung für den eigenen Bedarf in der Union haben;

Diese Regelung gilt nicht für eine Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt.

**Abbildung 13 – Nicht-personenbezogene Daten**



**Quelle:** Business2Community (2019)

Die Gewährleistung des freien Flusses nicht-personenbezogene Daten hat in der gesamten EU die folgenden Grundsätze:

- Der Grundsatz des freien Flusses nicht-personenbezogene Daten beseitigt ungerechtfertigte Beschränkungen der Datenlokalisierung, die von öffentlichen Behörden auferlegt wurden, und erhöht die Rechtssicherheit und das Vertrauen;
- Der Grundsatz der Datenverfügbarkeit für die zuständigen Behörden stellt sicher, dass die Daten für die Regulierungs- und Aufsichtskontrolle auch dann zugänglich bleiben, wenn sie grenzüberschreitend in der EU gespeichert oder verarbeitet werden.;
- Maßnahmen, um Anbieter von Cloud-Diensten zu ermutigen, selbstregulierende Verhaltenskodex für einen leichteren Wechsel des Anbieters und die Rückportierung von Daten auf hauseigene Server zu entwickeln, die bis Mitte 2020 umgesetzt werden müssen;
- Die Sicherheitsanforderungen an die Datenspeicherung und -verarbeitung bleiben weiterhin gültig, auch wenn Unternehmen Daten in einem anderen Mitgliedstaat speichern oder verarbeiten. Dasselbe gilt, wenn sie die Datenverarbeitung an Cloud-Service-Anbieter auslagern;
- Einheitliche Kontaktstellen in jedem Mitgliedstaat, die mit den Kontaktstellen der anderen Mitgliedstaaten und der Kommission in Verbindung stehen, um die wirksame Anwendung der neuen Vorschriften über den freien Verkehr nicht-personenbezogener Daten zu gewährleisten.

Die **DSGVO und die Verordnung über den freien Verkehr nicht-personenbezogene Daten werden zusammenwirken, um den freien Verkehr beliebiger Daten zu ermöglichen** und einen gemeinsamen europäischen Raum für Daten zu schaffen. Diese beiden Verordnungen schaffen zusammen Rechtssicherheit für Unternehmen und garantieren, dass personenbezogene und nicht-personenbezogene Daten innerhalb der EU frei zirkulieren können.

### **5.1. Freier Datenverkehr innerhalb der EU**

Anforderungen an die Datenlokalisierung sind verboten, es sei denn, sie sind aus

Gründen der öffentlichen Sicherheit unter Beachtung des Verhältnismäßigkeitsprinzips gerechtfertigt. Daher teilen die Mitgliedstaaten der Kommission unverzüglich jeden Gesetzesentwurf mit, der eine neue Datenlokalisierungsanforderung einführt oder Änderungen an einer bestehenden Datenlokalisierungsanforderung gemäß den in Artikel 5, 6 und 7 der Richtlinie (EU) 2015/1535 vorgesehenen Verfahren vornimmt.

Darüber hinaus stellt die **auf nicht-personenbezogene Daten angewandte Regelung** Folgendes sicher:

- **Freier Verkehr nicht-personenbezogener Daten über Grenzen hinweg:** Jede Organisation sollte in der Lage sein, Daten überall in der EU zu speichern und zu verarbeiten;
- **Die Verfügbarkeit von Daten für die regulatorische Kontrolle:** Die Behörden behalten den Zugang zu den Daten, auch wenn sie sich in einem anderen Mitgliedsstaat befinden oder in der Cloud gespeichert oder verarbeitet werden;
- Leichterer Wechsel von Cloud-Service-Anbietern für professionelle Anwender. Die Kommission hat damit begonnen, die Selbstregulierung in diesem Bereich zu erleichtern, indem sie die Anbieter ermutigt, Verhaltenskodizes zu entwickeln, die die Bedingungen betreffen, unter denen Nutzer Daten zwischen den Anbietern von Cloud-Diensten und zurück in ihre eigenen IT-Umgebungen portieren können;
- Volle Übereinstimmung und Synergien mit dem Cybersicherheitspaket und Klarstellung, dass alle Sicherheitsanforderungen, die bereits für Unternehmen gelten, die Daten speichern und verarbeiten, dies auch weiterhin tun werden, wenn sie Daten grenzübergreifend in der EU oder in der Cloud speichern oder verarbeiten..

Zusammen mit dieser Verordnung sieht die DSGVO bereits den freien Verkehr personenbezogener Daten vor. Bis zum 30. Mai 2021 haben die Mitgliedsstaaten auf der Grundlage des bestehenden Unionsrechts einige Regeln bezüglich der Anforderungen an die Datenlokalisierung festgelegt.

## 5.2. Übertragung von Daten

Die Europäische Kommission fördert und erleichtert die Entwicklung selbstregulierender

Verhaltensregeln auf Unionsebene, um zu einer wettbewerbsfähigen Datenwirtschaft beizutragen, die auf den Grundsätzen der Transparenz beruht, und erleichtert die Entwicklung selbstregulierender Kodex, um zu einer wettbewerbsfähigen Datenwirtschaft beizutragen.

### **5.3. Verfahren für die Zusammenarbeit zwischen Behörden**

Gemäß Artikel 7 soll jeder Mitgliedstaat eine einzige Kontaktstelle benennen, die mit den einzigen Kontaktstellen der anderen Mitgliedstaaten und der Kommission in Bezug auf die Anwendung dieser Verordnung in Verbindung steht. Dies bedeutet, dass die Mitgliedstaaten der Kommission die benannten einheitlichen Ansprechpartner und jede spätere Änderung mitteilen müssen.

### **5.4. Datenverfügbarkeit für zuständige Behörden**

In Bezug auf Artikel Nummer 5, berührt diese Verordnung nicht die Befugnisse der zuständigen Behörden, zur Erfüllung ihrer dienstlichen Aufgaben im Einklang mit dem Recht der Union oder dem nationalen Recht Zugang zu Daten zu verlangen oder zu erhalten. Nachdem eine zuständige Behörde um Zugang zu den Daten eines Nutzers ersucht hat, erhält sie keinen Zugang, und wenn nach dem Unionsrecht oder internationalen Vereinbarungen kein spezifischer Kooperationsmechanismus für den Datenaustausch zwischen den zuständigen Behörden verschiedener Mitgliedstaaten besteht, kann diese zuständige Behörde eine zuständige Behörde in einem anderen Mitgliedstaat um Unterstützung ersuchen, gemäß Artikel 7.

### **5.5. Strafen für Verstöße**

Diese Verordnung legt Sanktionen für einen Verstoß fest, die für verschiedene Verstöße unterschiedliche Strafen vorsehen (die gleichen Sanktionen, die nach DSGVO gelten, gelten auch für die ePR). Dies bedeutet, dass die Sanktionen bei schwereren Verstößen bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes betragen können, je nachdem, welcher Betrag höher ist.

Die Höhe der Bußgelder hängt in hohem Maße von einer Reihe mildernder Faktoren ab,

wie z.B. dem Ausmaß des Vorfalls, ob ein Regelverstoß durch eine vorsätzliche Handlung erfolgte und wie sorgfältig das Unternehmen bei der Verhinderung solcher Vorfälle vorgegangen ist.



## 6. Systematisierter Inhaltskatalog

**Cybersicherheit:** ist die Praxis des Schutzes von Systemen, Netzwerken und Programmen vor digitalen Angriffen. Diese Cyberangriffe zielen in der Regel darauf ab, auf sensible Informationen zuzugreifen, sie zu verändern oder zu zerstören, Geld von Benutzern zu erpressen oder normale Geschäftsprozesse zu unterbrechen.

**Datenschutzgesetz:** unabhängige öffentliche Behörden, die die Anwendung des Datenschutzgesetzes überwachen. Sie beraten in Datenschutzfragen und bearbeiten Beschwerden über Verstöße gegen die DSGVO und die einschlägigen nationalen Gesetze.

**Datenschutzbeauftragter:** die Person, die für die Überwachung und Anwendung der Datenschutzvorschriften in der Europäischen Kommission verantwortlich ist. Ein DSB ist ein Mitarbeiter innerhalb Ihrer Organisation, der für das Verständnis und die Einhaltung der Vorschriften in Ihrer Organisation verantwortlich ist. Der DSB stellt in Zusammenarbeit mit dem Europäischen Datenschutzbeauftragten die interne Anwendung der Datenschutzbestimmungen sicher.

**ePrivacy- Regelung:** Vorschlag der Europäischen Kommission zur Stärkung des Schutzes des Privatlebens der Bürger der Europäischen Union und zur Schaffung neuer Möglichkeiten für Unternehmen.

**DSGVO:** Regelung im EU-Recht zum Datenschutz und zur Privatsphäre für alle einzelnen Bürger der Europäischen Union und des Europäischen Wirtschaftsraums. Sie betrifft auch die Übermittlung von personenbezogenen Daten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

**Nicht-personenbezogene Daten:** elektronische Informationen, die nicht zu einer identifizierten oder identifizierbaren natürlichen Person zurückverfolgt werden können (oder als solche anonymisiert wurden).



**Personenbezogene Daten:** alle Informationen, die sich auf eine Person beziehen, die direkt oder indirekt identifiziert werden kann. Namen, Fotos, geografische Informationen, Web-Cookies, E-Mail-Adresse sind einige Beispiele für personenbezogene Daten.



## 7. Schlussfolgerung

Datenschutz und Cybersicherheit werden zu wesentlichen Werten für die Gesellschaft. Aus diesem Grund haben diese beiden Bereiche in letzter Zeit eine bedeutende rechtliche Entwicklung erfahren und sind in der EU stärker konsolidiert.

Die Regelung für den Umgang mit personenbezogenen Daten unterscheidet sich von der Regelung für die nicht-personenbezogenen Daten in den EU-Mitgliedstaaten. Die Vorschriften, die sich auf nicht-personenbezogene Daten und personenbezogene Daten beziehen, sind jedoch für alle Mitgliedstaaten gleich. In diesem Zusammenhang gilt die Verordnung (EU) 2018/1807 für den freien Verkehr nicht-personenbezogener Daten, während in Bezug auf den Datenschutz, wie in allen anderen EU-Jurisdiktionen, die Hauptregel die DSGVO ist. Zusammen mit der DSGVO wird die Verordnung über den freien Verkehr nicht-personenbezogener Daten zusammenwirken, um den freien Verkehr von Daten zu ermöglichen, der zu einem gemeinsamen europäischen Datenraum führt.

Darüber hinaus legt die ePR einige Regeln in Bezug auf den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation fest. Diese Verordnung gilt insbesondere für Anbieter von elektronischen Kommunikationsnetzen und -diensten und sollte am 25. Mai 2018 zusammen mit der DSGVO in Kraft treten, doch haben die anhaltenden Beratungen und die Lobbyarbeit die Anwendung dieser Verordnung verzögert. Die ePR enthält keine explizite Bestimmung hinsichtlich des anwendbaren nationalen Rechts, was zu Rechtsunsicherheit führt, welches Recht in einem grenzüberschreitenden Kontext gelten soll.

Die Datenschutz-Grundverordnung ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, enthält aber zahlreiche Öffnungsklauseln und lässt dem nationalen Gesetzgeber einen gewissen Spielraum.

## 8. Quellen

Business2Community (2019). Why User Data is the Next Big Deal in Digital? Abgerufen von <https://www.business2community.com/mobile-apps/why-user-data-is-the-next-big-deal-in-digital-02179282>.

Deloitte (2019). The DSGVO: Six Months after Implementation. Abgerufen von <https://www2.deloitte.com/bg/en/pages/legal/articles/DSGVO-six-months-after-implementation-2018.html>.

EU DSGVO.ORG (2019). The EU General Data Protection Regulation (DSGVO) is the most important change in data privacy regulation in 20 years. Abgerufen von <https://euDSGVO.org/>.

European Commission (2019). Complete guide to DSGVO compliance. Abgerufen von <https://DSGVO.eu/>.

European Commission (2019). Data protection under DSGVO. Abgerufen von [https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-DSGVO/index\\_en.htm#shortcut-3-who-monitors-how-personal-data-is-processed-within-a-company](https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-DSGVO/index_en.htm#shortcut-3-who-monitors-how-personal-data-is-processed-within-a-company).

European Commission (2019). Eurobarometer on ePrivacy. Abgerufen von <https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy>.

European Commission (2019). Free flow of non-personal data. Abgerufen von <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>.

European Commission (2019). General Data Protection Regulation: one year on. Abgerufen von: [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_19\\_2610](https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610).

European Commission (2019). Proposal for a regulation on privacy and electronic communications. Abgerufen von <https://ec.europa.eu/digital-single->

[market/en/news/proposal-regulation-privacy-and-electronic-communications](https://www.market/en/news/proposal-regulation-privacy-and-electronic-communications).

i-Scoop (2019). Data processing principles: the 9 DSGVO principles relating to processing personal data. Abgerufen von <https://www.i-scoop.eu/DSGVO/DSGVO-personal-data-processing-principles/>.

ITPRO (2019). ePrivacy Regulation: What is it and how does it affect me? Abgerufen von <https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me>.

Serve IT (2017). DSGVO for developers - data subject rights. Abgerufen von <https://www.serveit.com/DSGVO-for-developers-data-subject-rights/>.