Markus Näf

WEKA

Anwendbarkeit der EU-DSGVO in der Schweiz

Ein Datenschutzleitfaden für Schweizer Unternehmen

BOOKS BUSINESS BOOKS

Ein Problem? ***Kein Problem!***

CIP-Kurztitelaufnahme der deutschen Bibliothek

Anwendbarkeit der EU-DSGVO in der Schweiz

Herausgeber: Markus Näf

Projektleitung: Junes Babay

WEKA Business Media AG
Hermetschloostrasse 77, CH-8048 Zürich
Telefon 044 434 88 88, Telefax 044 434 89 99
www.weka.ch

Zürich • Kissing • Paris • Wien

ISBN 978-3-297-02126-2

1. Auflage 2019

Druck: CPI books GmbH, Leck, Layout: Dimitri Gabriel, Satz: Peter Jäggi

Autor

Markus Näf

ist als Rechtsanwalt tätig und spezialisiert auf Informatik- und Datenschutzrecht. Er hat als zertifizierter Projektmanager (Certified Senior Project Manager IPMA Level B) zahlreiche Informatikprojekte selbst geleitet und umgesetzt oder rechtlich begleitet. Er ist Lehrbeauftragter für Informatikrecht und Projektmanagement an der Fachhochschule St. Gallen (www.fhsg.ch) sowie Verwaltungsrat mehrerer Gesellschaften.

Inhaltsübersicht

1. Einleitung

1. Einleitung

Die Datenschutz-Grundverordnung im Besonderen und die Datenschutzgesetze ganz allgemein beziehen sich immer nur auf den Schutz von Daten von natürlichen Personen.[1] Die DSGVO spricht von **«personenbezogenen Daten»**. Dieser Begriff ist in Art. 4 Ziff. 1 DSGVO wie folgt konkretisiert:

> *«Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‹betroffene Person›) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.»*

Der Begriff der Personendaten ist sehr weit gefasst und umfasst zum Beispiel auch die Gerätenummer des Mobiltelefons oder die IP-Adresse der Internetverbindung. Die Datenschutzregulierungen schreiben weitergehend auch Massnahmen zur Informatiksicherheit vor, indem sie einen angemessenen Schutz von elektronischen Personendaten nach dem aktuellen Stand der Technik vorschreiben.

In Bezug auf die Aufbewahrung und Archivierung von Daten müssen zusätzlich auch die Bestimmungen aus dem Handelsrecht und verschiedener Spezialgesetze, wie zum Beispiel der Geschäftsbücherverordnung oder dem Bundesgesetz über die elektronische Signatur einbezogen werden.

Es gilt zusätzlich zu beachten, dass in Unternehmen neben den Personendaten weitere, meist noch viel wichtigere Daten vorhanden sind, die schätzenswerte Geschäftsgeheimnisse darstellen. Zum Beispiel Forschungsdaten, Entwicklungsdaten, Produktedaten und vieles mehr. Diese fallen aber nicht unter das Datenschutzrecht.

Es ist daher empfehlenswert, beim Thema Datenschutz eine Gesamtbetrachtung vorzunehmen und auch diese Daten und Themen miteinzubeziehen.

1 Das aktuelle DSG umfasst auch den Schutz von Personendaten juristischer Personen. Dieser Schutzumfang wird mit der Revision jedoch aufgehoben, und es werden auch nur noch Daten von natürlichen Personen einbezogen.

1.1 Entwicklungen im Datenschutz

Das schweizerische Datenschutzgesetz (DSG) wurde am 19. Juni 1992 verabschiedet und am 1. Juli 1993 in Kraft gesetzt. Es war damals geprägt von den staatlichen Datensammlungen, der sog. Fichenaffäre. Das DSG regelt daher in einem ersten Teil die Datenbearbeitung durch Bundesbehörden und in einem zweiten Teil durch private Personen. Daneben regeln die kantonalen Datenschutzgesetze die Datenbearbeitung durch kantonale Instanzen und Gemeinden. Diese sind auf Unternehmen jedoch nicht anwendbar, ausgenommen natürlich wenn sie im Auftrag von Kantonen oder Gemeinden Daten bearbeiten. Die Entwicklung der elektronischen Datenverarbeitungen machten mehrfach Revisionen des DSG notwendig.

Der Europarat hat eine Verbesserung des Datenschutzes mit der Überarbeitung der Konvention 108 (ERK 108 – Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten[2]) beschlossen. Dieser war Auslöser für Evaluation des Datenschutzes in der Schweiz und in der EU und hat zu den neuen Datenschutzregulierungen geführt.

In der Schweiz wird derzeit die Botschaft des Bundesrats zur Revision des Datenschutzgesetzes in den parlamentarischen Kommissionen beraten. Der Entwurf muss sich sehr stark an der DSGVO orientierten, da die Schweiz für einen einfachen Datenaustausch mit den EU-Ländern einen gleichwertigen Datenschutz wie die EU sicherstellen muss und natürlich auch die ERK 108 erfüllen muss. Das schweizerische Datenschutzgesetz wird voraussichtlich Mitte 2020 in Kraft treten. Da in der Revision des schweizerischen Datenschutzgesetzes die meisten Bestimmungen aus der DSGVO übernommen werden, können Unternehmen mit der Umsetzung der DSGVO voraussichtlich auch die zukünftigen Bestimmungen des DSG problemlos erfüllen. Ein Zuwarten mit der Umsetzung bringt daher kaum Vorteile.

Die neue Datenschutzregulierung wird durch drei neue Stossrichtungen geprägt:

1. Erstens sind zum Schutz der Konsumenten pauschale Einwilligungen in zukünftige Datenbearbeitungen nicht mehr möglich, sondern es gibt detaillierte Vorschriften über die Form der Aufklärung und der Einwilligung (informed consent), und diese ist nur noch im konkreten Einzelfall möglich.
2. Zweitens müssen aufgrund der Beweislastumkehr für die Rechtmässigkeit der Datenbearbeitung zahlreiche formale Vorschriften und Dokumentationspflichten durch das Unternehmen erfüllt werden.
3. Drittens erhalten die Aufsichtsbehörden umfassende Kontrollrechte, und ein weitgehender Bussen- und Strafkatalog ermöglicht die Sanktionierung fehlbarer Unternehmen.

2 www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108

Diese Verbotskultur der Datenbearbeitung steht teilweise im Widerspruch zu sehr liberalen Regelungen ausserhalb von Europa.

Einer dieser Konfliktbereiche ist der Datenaustausch mit Unternehmen in den Vereinigten Staaten, was aufgrund der Tatsache besonders relevant ist, da acht der zehn grössten Technologie-Unternehmen der Welt aus den USA stammen (die anderen beiden aus der Volksrepublik China). Aus Sicht der Schweiz und der EU verfügen die USA nicht über einen gleichwertigen Datenschutz. Daher ist der Austausch von Personendaten an zusätzliche Vorschriften geknüpft und nicht einfach formlos möglich. Dies wurde mit dem Staatsvertrag über das Privacy-Shield-Abkommen ausformuliert. Die USA ermöglichen aber über den Stored Communication Act oder über den erst am 23. März 2018 beschlossenen Cloud Act (Clarifying Lawful Overseas Use of Data Act) den Behörden Zugriff auf Daten bei US-Unternehmen auch ausserhalb der USA (so z.B. in Rechenzentren in Europa). Diese Entwicklungen sind daher sorgfältig zu beobachten.

1.2 Aufbau des Praxisleitfadens

Dieser Praxisleitfaden soll Ihnen eine komprimierte Übersicht über die Europäische Datenschutz-Grundverordnung geben und jeweils den Handlungsbedarf und wenn immer möglich auch ein Anwendungsbeispiel für ein Schweizer Unternehmen aufzeigen.
Im Buch werden Hilfestellungen mit folgenden Symbolen angezeigt:

	Mit diesem Symbol werden praktische Umsetzungstipps zum jeweiligen Thema bezeichnet.
	Dieses Symbol bezeichnet praktische Umsetzungshilfen und Vorlagen im Anhang des Buches.
	Dieses Symbol zeigt hilfreiche Internetlinks auf Seiten mit weitergehenden Informationen und hilfreichen Umsetzungshilfen.

Die Darstellung kann jedoch zum heutigen Zeitpunkt in keinem Fall abschliessend sein, da aufgrund der gemeinsamen Regulierung und Zustimmung aller 28 EU-Länder die Bestimmungen in der Verordnung teilweise sehr allgemein formuliert wurden. Die Umsetzungsbestimmungen und konkrete Anwendungsfragen werden nun laufend durch die Europäische Datenschutzgruppe zusammen mit den Datenschutzbehörden der einzelnen Länder konkretisiert.

Die datenschutzrechtlichen Konsequenzen eines Austritts von Grossbritannien aus der EU sind noch nicht erfasst und dargestellt.

Dies bedeutet aber gleichzeitig, dass die Aufsichtsbehörden auch die Umsetzungsbestimmungen formulieren, was tendenziell eher zu einer weitgehenden Auslegung der Bestimmungen führt. Die Korrektur und allenfalls auch eine Einschränkung der ausufernden Auslegung wir erst in der Zukunft durch Gerichtsentscheide erfolgen. Aufgrund der bisher kurzen Anwendungsdauer gibt es noch keine Gerichtspraxis.

WEITERGEHENDE INFORMATIONEN

Europäischer Datenschutzausschuss:
https://edpb.europa.eu/edpb_de

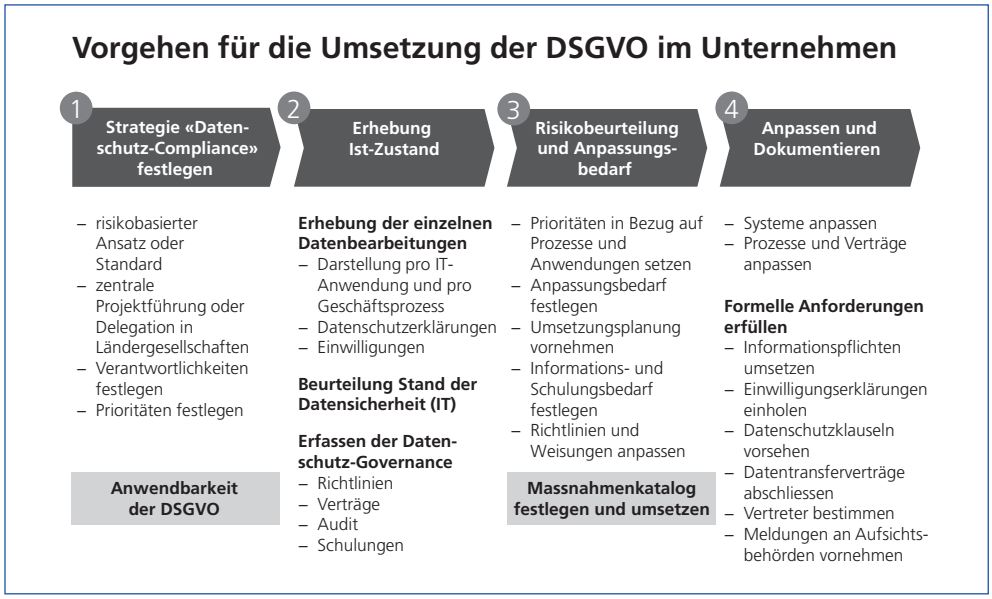
Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter:
www.edoeb.admin.ch/edoeb/de/home/dokumentation/rechtliche-grundlagen/Datenschutz%20-%20International/DSGVO.html

Die DSGVO gibt heute noch nicht zu allen Anwendungsfragen eine Antwort. Erst die Rechtsprechung wird die konkrete Auslegung klären. Die Anwendung und Umsetzung der DSGVO ist daher im Einzelfall zu beurteilen und kann sich in Zukunft auch noch ändern. Die DSGVO sieht daher auch eine risikobasierte Umsetzung vor. Das heisst, das Unternehmen hat eine Risikoeinschätzung in Bezug auf die Persönlichkeitsrechte der von der Datenbearbeitung betroffenen Personen vorzunehmen und darauf gestützt angemessene, aber nicht alle möglichen Schutzmassnahmen zu treffen.

1.3 Handlungsfelder und Vorgehen bei der Umsetzung in Schweizer Unternehmen

Die DSGVO verlangt eine risikobasierte Umsetzung. Die Regelungen enthalten in einzelnen Bereichen keine exakten Vorgaben für eine Umsetzung, sondern es ist eine Beurteilung vorzunehmen, und es sind adäquate Massnahmen umzusetzen.

Dabei kann nach folgendem Schema vorgegangen werden:



Grundsätzlich ist in einem ersten Schritt zu prüfen, ob die DSGVO auf ein Schweizer Unternehmen anwendbar ist [siehe dazu Kapitel 2.1].

In einem zweiten Schritt ist eine Übersicht über die bestehenden Datenbearbeitungen, Geschäftsprozesse, Applikationen und Datenbearbeitungen zu erstellen.

In einem dritten Schritt ist eine Risikobeurteilung vorzunehmen, und es sind die konkreten Umsetzungsmassnahmen festzulegen.

PRAXISTIPP

Checkliste von möglichen Themenfeldern für die Umsetzung

- ❑ Anwendbarkeit von ausländischen und/oder nationalen Datenschutzbestimmungen
- ❑ Datenschutzerklärung und Nutzungsbedingungen Internetseite
- ❑ Bestehende Privacy Policy/Datenschutzweisungen
- ❑ Bestehende Datenschutzklauseln in Verträgen und Allgemeinen Geschäftsbedingungen
- ❑ Übersicht über Datenbearbeitungen, Applikationen und Prozesse
- ❑ Rechtsgrundlage für die Bearbeitung von Personendaten
- ❑ Einwilligung in die Bearbeitung Daten
- ❑ Prozesse für die Erfüllung der Betroffenenrechte (Auskunft, Löschung etc.)
- ❑ Beschäftigtendatenschutz
- ❑ Zulässigkeit einer Datenweitergabe an Dritte
- ❑ Auftragsverarbeiter – erforderliche Vereinbarungen
- ❑ Anforderungen an Datenübermittlung in Drittländer
- ❑ Pflicht zur Führung von Verarbeitungsverzeichnissen (Verantwortlicher und/oder Auftragsverarbeiter)
- ❑ Notwendigkeit für die Ernennung eines betrieblichen Datenschutzbeauftragten
- ❑ Notwendigkeit für die Ernennung eines Vertreters in der EU
- ❑ Meldungen an die zuständigen und/oder betroffenen Datenschutzaufsichtsbehörden
- ❑ Prozess Data Breach Notification
- ❑ Notwendigkeit einer Datenschutz-Folgenabschätzung
- ❑ Dokumentation technische und organisatorische Massnahmen (Datensicherheit)
- ❑ Prüfen von Zertifizierungen
- ❑ Regelung der elektronischen und physischen Archivierung

In einem vierten Schritt sind die Massnahmen nach Prioritäten zu realisieren. Dabei sollten die Themen mit hoher Sichtbarkeit, wie zum Beispiel die Internetseite, als Erstes umgesetzt werden.

Die Einhaltung der Datenschutzbestimmungen und die Prozesse sollten einmal pro Jahr überprüft werden.

1.4 Risiken bei Untätigkeit

Unternehmen setzen sich erheblichen Risiken aus, wenn sie pflichtwidrig die Vorschriften der DSGVO nicht umsetzen. Dabei stehen wahrscheinlich weniger die Sanktionen von Aufsichtsbehörden im Vordergrund, da diese kaum die Kapazitäten haben, jedes noch so kleine Unternehmen zu prüfen und zu verfolgen. Nach dem risikobasierten Ansatz ist aber auch hier davon auszugehen, dass Unternehmen, deren Geschäftsmodell die Bearbeitung von Personendaten ist, eher im Fokus stehen als Unternehmen, die nur ab und zu Waren in die EU liefern.

Die maximalen Sanktionen können ein Unternehmen jedoch empfindlich treffen, können sie doch bis 4% des globalen Umsatzes eines Unternehmens oder EUR 20 Mio. betragen (siehe dazu auch Strafbestimmungen in Kapitel 12.5).

Unangenehmer dürften jedoch für Unternehmen die neuen direkten Haftungsrisiken bei Datenschutzverletzungen sein und die damit verbundenen Reputationsrisiken. Zudem ist zu beachten, dass heute internationale Handelsverträge häufig sogenannte «Compliance-Klauseln» enthalten. Diese berechtigen einen Vertragspartner bei Verstössen gegen die Compliance – was ein Datenschutzverstoss respektive die Nichteinhaltung der DSGVO ist, den Vertrag ausserordentlich zu kündigen und oftmals auch eine Konventionalstrafe geltend zu machen.

Bei Internetseiten oder Konsumentenverträgen, die nicht datenschutzkonform sind, besteht ein hohes Risiko für kostenpflichtige Abmahnungen von Konsumenten, Konsumentenschutzorganisationen oder Mitbewerbern. Eine solche Abmahnindustrie existiert vor allem in Deutschland und teilweise in Österreich. Unternehmen sind daher gut beraten, ihren Internetauftritt in Bezug auf diese Märkte datenschutzkonform zu gestalten.

2. Europäische Datenschutz-Grundverordnung (EU-DSGVO)

2. Europäische Datenschutz-Grundverordnung (EU-DSGVO)

Das Europäische Parlament hat am 14. April 2016 die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung oder DSGVO) verabschiedet.[1] Die Verordnung ist nach einer zweijährigen Übergangszeit seit dem 25. Mai 2018 in allen 28 Ländern der Europäischen Union direkt anwendbar. Es braucht daher keine Umsetzung in der nationalen Gesetzgebung in den einzelnen EU-Ländern.

Trotzdem können die EU-Länder weiterhin eigene Datenschutzgesetze erlassen, da die DSGVO rund 83 Regulierungsvorbehalte kennt, bei denen die Länder weitergehende Regelungen erlassen können. Ein solches Beispiel ist die Pflicht, einen Datenschutzbeauftragten zu ernennen (siehe Kapitel 7.1).

Der EWR hat am 6. Juli 2018 die Übernahme der DSGVO in das EWR-Abkommen beschlossen. Damit wird die DSGVO seit dem 20. Juli 2018 auch für die EWR-/EFTA-Staaten Liechtenstein, Norwegen und Island unmittelbar anwendbar.

WEITERGEHENDE INFORMATIONEN

Die Datenschutzstelle des Fürstentums Liechtenstein veröffentlicht auf ihrer Internetseite praktische Informationen zur DSGVO und insbesondere auch Muster für Datenschutzerklärungen, Einwilligungserklärungen oder allgemeine Vorlagen:
https://www.datenschutzstelle.li/

Liechtensteinische Datenschutzkommission als unabhängige Beschwerdeinstanz:
http://www.datenschutzkommission.li/

2.1 Anwendbarkeit der DSGVO auf Schweizer Unternehmen

Aufgrund des Marktortprinzips hat die DSGVO auch extraterritoriale Wirkung und ist auch auf Unternehmen ausserhalb der EU anwendbar. Diese Verordnung hat daher auf eine Vielzahl von Schweizer Unternehmen direkte Auswirkungen.

1 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=de

2.1.1 Räumlicher Anwendungsbereich (Art. 3 DSGVO)

Der räumliche Anwendungsbereich umfasst das Kriterium der Niederlassung, das heisst der Ort der Niederlassung des Verantwortlichen oder des Auftragsverarbeiters von personenbezogenen Daten. Ein Datenverarbeiter in den EU-Ländern und den EWR-Ländern Liechtenstein, Norwegen und Island fällt damit automatisch unter die DSGVO. Damit ist klar, sobald ein Schweizer Unternehmen eine Niederlassung oder eine Betriebsstätte in diesen Ländern hat, fällt es unter den Anwendungsbereich.[2]

Das zweite Kriterium ist der Zielmarkt, das heisst der Wohnort der von der Datenbearbeitung betroffenen Personen. Damit findet die Verordnung auch Anwendung auf Unternehmen ausserhalb der EU, wenn diese

a) betroffenen Personen in der EU oder den EWR-Ländern Waren oder Dienstleistungen anbieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist, oder
b) das Verhalten betroffener Personen beobachten, soweit ihr Verhalten in der Union erfolgt. Unter diese Verhaltensbeobachtung fällt vor allem auch die Beobachtung des Verhaltens von Internetnutzerinnen und -nutzern mittels Trackern und Cookies.

Im Grundsatz findet die DSGVO immer dann Anwendung, wenn eine sich in einem Mitgliedstaat der EU aufhaltende Person, unabhängig von ihrer Staatsangehörigkeit oder ihrem Wohnsitz, direkt von einer Datenbearbeitung betroffen ist. Es gibt aber dazu einige Ausnahmen. Bei der Beurteilung, ob die Verordnung zur Anwendung kommt, ist stets der Einzelfall und insbesondere die Absicht des Verantwortlichen zu berücksichtigen, Personen im Gebiet der Union Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten.

2.1.2 Sachlicher Anwendungsbereich

Grundsätzlich findet die DSGVO Anwendung auf die Bearbeitung von personenbezogenen Daten von natürlichen Personen. Die Verordnung gilt jedoch nicht für die Verarbeitung von personenbezogenen Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschliesslich Name, Rechtsform oder Kontaktdaten der juristischen Personen.[3] Damit ist auch klar, dass die reine Bearbeitung von Kunden- oder Lieferantendaten im Business-to-Business-Geschäft mit Firmen nicht unter die DSGVO fällt. Abzugrenzen ist davon jedoch hier wieder die Erfassung von Kundenprofilen der Kontaktpersonen der juristischen Person.

2 Der Begriff der Niederlassung ist gemäss dem Entscheid C-230/14 des EuGH weitgehend auszulegen. In Erwägungsgrund 22 wird klargestellt, dass eine Niederlassung die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraussetzt. Die Rechtsform einer solchen Einrichtung ist dabei nicht ausschlaggebend.

3 Erwägungsgrund 14 zur DSGVO.

Die Verordnung findet keine Anwendung auf die Bearbeitung von Personendaten durch natürliche Personen zu rein persönlichen und familiären Zwecken.

2.1.3 Anwendungsfälle

Die nachstehenden Anwendungsfälle sollen anhand von Beispielen erläutern, ob die DSGVO auf ein Unternehmen oder einen Sachverhalt anwendbar ist:

Fallbeschreibung	Anwendbarkeit
Auftragsverarbeiter in der EU Ein Schweizer Unternehmen beauftragt in der EU einen IT-Dienstleister (Auftragsverarbeiter) mit der Datenbearbeitung. Das Schweizer Unternehmen unterliegt in diesem Fall nicht der DSGVO. Der Auftragsverarbeiter in der EU unterliegt jedoch den Vorschriften der DSGVO, unabhängig davon, ob er Daten von Betroffenen in der Schweiz oder in der Union verarbeitet. Er muss sowohl die in der Verordnung festgelegten besonderen Pflichten der Auftragsverarbeiter als auch die sich aus dem schweizerischen Recht ergebenden Anforderungen nach Art. 10a DSG einhalten.	nein
Auftragsverarbeiter in der Schweiz Ein Unternehmen in der EU beauftragt einen Schweizer IT-Dienstleister (Auftragsverarbeiter) mit der Datenverarbeitung. Das Unternehmen bearbeitet damit Daten von Personen aus der EU, und die DSGVO ist auf den Schweizer Dienstleister anwendbar. Jedoch nur auf diejenigen Bereiche, welche die Datenbearbeitung für den Auftraggeber in der EU betreffen.	ja
Detailhändler in der Schweiz Ein Unternehmen mit Sitz in der Schweiz bietet seine Waren nur in der Schweiz an. Ab und zu kommen Personen mit Wohnsitz in der EU und kaufen Waren ein. Wenn eine Person aus der EU in die Schweiz kommt und hier Waren oder Dienstleistungen einkauft, fällt das Unternehmen deswegen nicht unter die DSGVO. Das Schweizer Unternehmen darf auch die Kontaktdaten des Käufers erfassen und speichern.	nein
Waren oder Dienstleistungsangebote in die EU Ein in der Schweiz ansässiges Unternehmen verkauft Uhren über einen Online-Shop an Personen mit Wohnsitz in einem oder mehreren EU-Ländern. Die DSGVO ist anwendbar, weil das Schweizer Unternehmen seine Waren Personen in der EU anbietet.	ja
Schweizer Verein bietet Mitgliedschaften an Personen in der EU an Es handelt sich hier ebenfalls um ein Dienstleistungsangebot an Personen in der EU. Die DSGVO ist anwendbar.	ja
Online-Auftritt eines Hotels Ein Hotelier im Engadin erstellt von seinen italienischen, schwedischen, deutschen und polnischen Gästen Profile, um ihnen Angebote für andere Aufenthalte machen zu können. Die DSGVO ist anwendbar, soweit das Profil auf der Grundlage eines Verhaltens in der EU erstellt wird.	ja