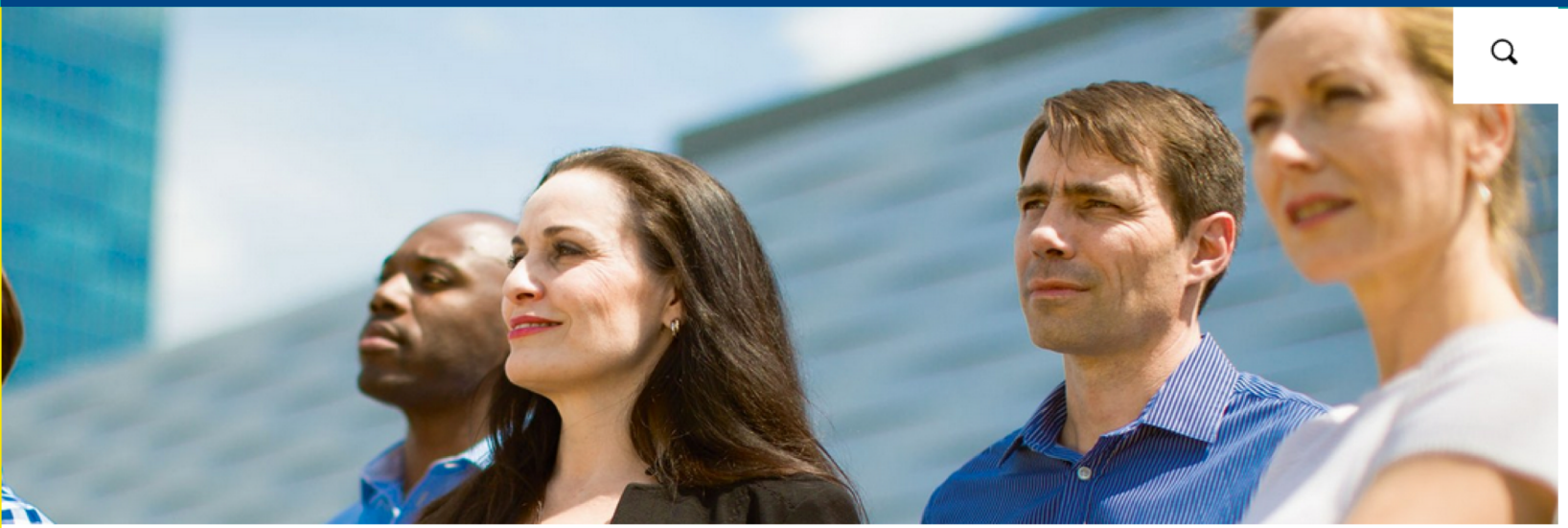
Fachhochschule Nordwestschweiz FHNW



Weiterbildung ▸ Wirtschaft

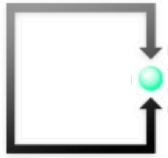
Praxisseminar Datenschutzverordnung DSGVO (Data Privacy)

Die neue EU-DSGVO kennen lernen, beurteilen und effizient umsetzen

Praxisseminar DSGVO

Nutzen für die Praxis

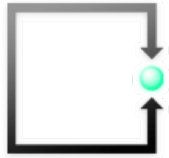
- Sie kennen die neuen Datenschutz-Anforderungen und deren Folgen.
- Sie wissen, wie Sie
  - eine **Datenschutzerklärung** formulieren
  - nach welchen Prioritäten Sie Ihr **Unternehmen rechtlich absichern**
  - eine **Prozessdokumentation** erstellen
  - die **Datenschutz-Folgeabschätzung** durchführen
  - welche **organisatorischen oder technischen Massnahmen** notwendig sein können
  - den **Datenschutzbeauftragten** oder einen **EU- Datenschutzvertreter** einsetzen
  - **Informations-, Berichtigungs- oder Löschbegehren** korrekt erfüllen
  - **Meldepflichten bei Datenschutzverletzungen** erfüllen



Die Inhalte des Seminars

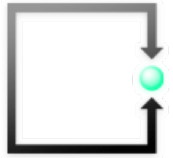
- Überblick über Neuerungen im Datenschutz in der EU und der Schweiz
- Anwendungsbereich der Vorschriften für EU- und Schweizer Unternehmen
- Neue Pflichten der Unternehmen für die Erfüllung des Datenschutzes
- Alte und neue Rechte der Betroffenen
- Rollen und Einbindung von Partner-Unternehmen und Lieferanten
- Implementierung der Datenschutzvorschriften
- Projektschritte und Pflege im operativen Bereich

- Möglichkeit für Fragen und Diskussion

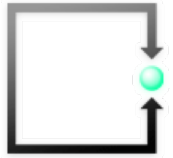


Inhaltsübersicht

1. Ausgangslage und Ziele der DSGVO
2. Status CH-Datenschutz-Gesetzgebung
3. Compliance und gesetzliche Verantwortung von VR und GL
4. Die wichtigsten Aspekte für Unternehmen
5. Die (neuen) Begriffe
6. Örtlicher und sachlicher Anwendungsbereich der DSGVO
7. Das Standard-Datenschutzmodell SDM
8. DS-Pflichten der Unternehmen und die Sanktionen
9. DS-Rechte der Betroffenen
10. Der beigezogenen Datenverarbeiter
11. Das Projektvorgehen
12. Spezialfragen



1
Ausgangslage und Ziele der DSGVO



Neues Datenschutzrecht in der EU und CH

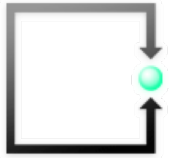
www.

Einleitung

Entstehungsgeschichte

- Datenschutzrecht stammt in EU und CH aus 1995
- Januar 2012: EU-Kommission schlägt Massnahmen vor zur Aktualisierung und Modernisierung der Datenschutz-Richtlinie 95/46/EG und des Rahmenbeschlusses (polizeiliche und justizielle Zusammenarbeit) 2008/977/JI

- **Ziel:**
  EU-weit einheitliche, an das digitale Zeitalter angepasste Regeln für alle EU-Staaten, um Rechtssicherheit zu verbessern und Vertrauen von Bürgerinnen und Bürger in den digitalen Binnenmarkt zu stärken.



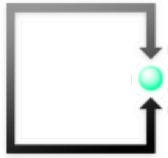
Die DSGVO

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

- Am 24.4.2016 vom EU-Parlament angenommen.
- Tritt am 25.5.2018 in Kraft
- Gilt ab diesem Datum für alle Akteure, die auf dem Gebiet der EU tätig sind

- EU-Verordnung ist in Gesamtheit verbindlich
- EU-Verordnung ist in jedem EU-Land unmittelbar anwendbar (keine nationalen Gesetz mehr notwendig)
- **Aber zahlreiche Ausnahmetatbestände** (Öffnungsklauseln) **eingeführt** (z.B. Ausdehnung auf juristische Personen möglich -> Österreich)

Beilage 01



Verordnungstext mit Erwägungen

http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679

I

(Gesetzgebungsakte)

VERORDNUNGEN

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)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

auf Vorschlag der Europäischen Kommission,

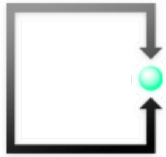
nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Stellungnahme des Ausschusses der Regionen ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:



Verordnungstext mit Erwägungen (2)

in Erwägung nachstehender Gründe:

(1) Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta") sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

(3) Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (4) ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.

Verordnungstext mit Erwägungen (3)

(172) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 konsultiert und hat am 7. März 2012 ([1]) eine Stellungnahme abgegeben.

(173) Diese Verordnung sollte auf alle Fragen des Schutzes der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten Anwendung finden, die nicht den in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([2]) bestimmte Pflichten, die dasselbe Ziel verfolgen, unterliegen, einschließlich der Pflichten des Verantwortlichen und der Rechte natürlicher Personen. Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten —

([1]) ABl. C 192 vom 30.6.2012, S. 7.
([2]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Verordnungstext mit Erwägungen (4)

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

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

Artikel 2

Sachlicher Anwendungsbereich

(1) Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

(2) Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

Verordnungstext mit Erwägungen (5)

Artikel 98

Überprüfung anderer Rechtsakte der Union zum Datenschutz

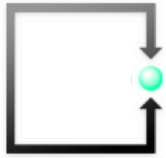
Die Kommission legt gegebenenfalls Gesetzgebungsvorschläge zur Änderung anderer Rechtsakte der Union zum Schutz personenbezogener Daten vor, damit ein einheitlicher und kohärenter Schutz natürlicher Personen bei der Verarbeitung sichergestellt wird. Dies betrifft insbesondere die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung solcher Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union und zum freien Verkehr solcher Daten.

Artikel 99

Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.



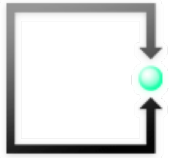
DSGVO – direkte Anwendbarkeit

- DSGVO hat 99 Artikel

- EU-Verordnung gilt direkt für alle EU-Länder gleich
- Alle EU-Einwohner können sich darauf berufen

- Nationale Ergänzungsgesetze (DE: Bundesdatenschutz-gesetz – BDSG 2018)
- Nationale Rechtsprechung (Erste Instanz)
- EuGH– Europäischer Gerichtshof sorgt für gleiche Auslegung in EU

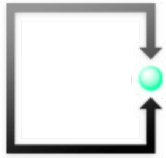
- Aber 69 Nationale Öffnungsklauseln vorgesehen



DSGVO – Nationale Öffnungsklauseln

- Spielräume bei der Datenverarbeitung auf gesetzlicher Ebene
- Spielräume bei der Verarbeitung besonders geschützter Daten
- Spielräume bei Betroffenenrechten
- Spielräume bei der Einwilligung
- Spielräume bei Auftragsverarbeitern
- Spielräume bei der Ausgestaltung der Datenschutzbehörden
- Spielräume bei den Befugnissen der Datenschutzbehörden
- Spielräume bei der Vertreten von Betroffenen durch NGOs
- Spielräume bei der Auflösung von Grundrechtskonflikten
- Spielräume im Arbeitsverhältnis

Beilage 05



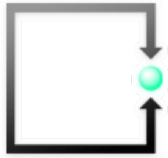
DSGVO – Nationale Öffnungsklauseln (2)

- Spielräume im Arbeitsverhältnis

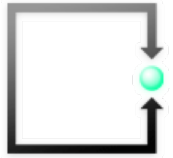
➢ Art. 9 Abs 2 lit b:
  - **Arbeits- und Sozialrecht** jedes Staates als Rechtsgrundlage für die Verarbeitung sensibler (Arbeitnehmer-) Daten

➢ Art. 88:
  - Beschäftigungskontext: **Spezifischere Vorschriften** zur Gewährleistungen des Schutzes von Beschäftigten **erlaubt**
  - durch Rechtsvorschriften oder Kollektivvereinbarungen (Erwägungs-Grund 155 Satz 1: „einschliesslich Betriebsvereinbarungen“)

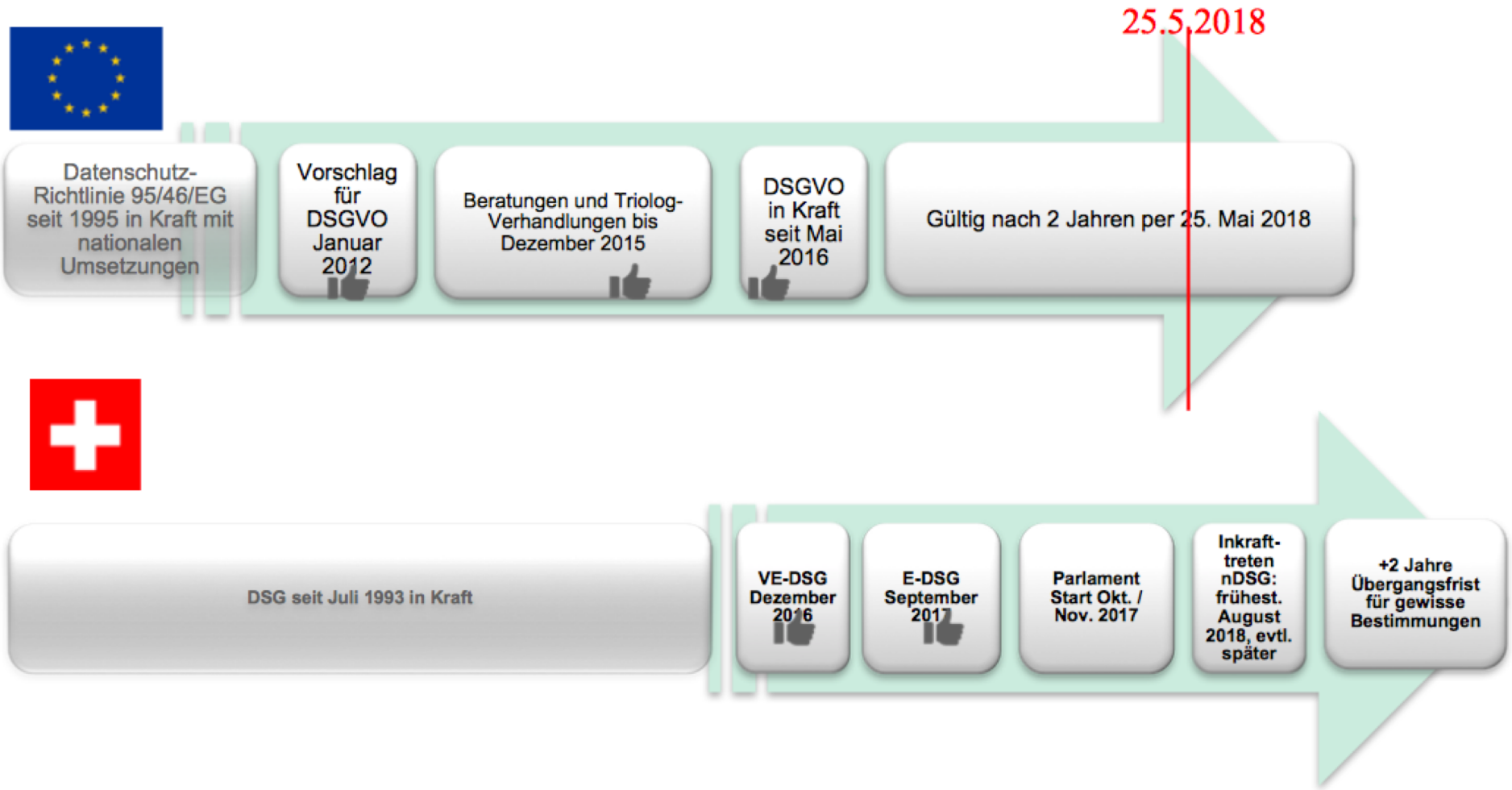
Vgl. separate Beilage 06



2
Status CH-Datenschutzgesetzgebung



Umsetzung in der CH



Umsetzung in der CH (2)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature] [QR Code]

Anhang *Vorentwurf*

Bundesgesetz über den Datenschutz
(Datenschutzgesetz, DSG)

vom …

Beilage 03

- Am 21. Dezember 2016 schickt der Bundesrat den Vorentwurf zu einer Totalrevision des DSG und zur Änderung weiterer Erlasse zum Datenschutz in die Vernehmlassung (Medienmitteilung).

- **Vernehmlassung zum Gesetzesentwurf lief bis 4. April 2017**
- **Botschaft des Bundesrates an das Parlament am 15.9.2017**
- **Behandlung im Nationalrat und Ständerat steht noch aus (Trennung)**
- **Inkrafttreten in der Schweiz circa ab 2019 zu erwarten**
- **Evtl. mit Übergangsfrist von 2 Jahren**
- **gemäss Interview des Infochefs BJ: Ziel August 2018 (?)**

SRF 3 Info 3 30-06-2017: podcasts.srf.ch/world/audio/Info-3_30-06-2017-1200.1498818184829.mp3

Umsetzung in der CH (3)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

17.059

Botschaft
zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz

vom 15. September 2017

Umsetzung in der CH (4)

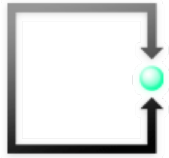
Schweiz riskiert bei Datenschutz neuen Konflikt mit der EU

Weil Bern bei der Modernisierung der Datenschutzgesetze zu langsam vorwärtskommt, könnte Brüssel den Marktzugang für Schweizer Unternehmen erschweren.

Die Verwaltung will wegen der EU «aufs Gaspedal» drücken.

Eigentlich hätte der Bundesrat nach der Frühjahrssession Verhandlungen mit der EU über die Erneuerung der Anerkennung aufnehmen wollen. Die Voraussetzung dafür wäre, dass das Parlament mit den Beratungen der Revision des Schweizer Datenschutzgesetzes begonnen hat und absehbar ist, wie es die Vorgaben der EU umsetzen will.

Doch dieser Plan dürfte nicht aufgehen. Eine klare Mehrheit in der vorberatenden Kommission des Nationalrats widersetzt sich. Sie hat letzte Woche beschlossen, die Revision aufzusplitten. Der Schengen-Teil soll zuerst beraten werden. Der zweite Teil, der für die Gleichwertigkeitsanerkennung relevant ist, danach.



Umsetzung in der CH (5)

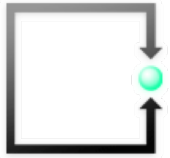
Video: Bundesrat will den Datenschutz verbessern

Bundesrätin Simonetta Sommaruga erklärt, was dies für den Kunden und die Unternehmen bedeutet. (September 2017)

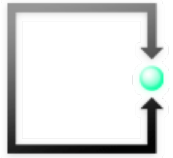
Beilage 02

https://www.tagesanzeiger.ch/schweiz/standard/Schweiz-riskiert-bei-Datenschutz-neuen-Konflikt-mit-der-EU/story/13706225

3
Compliance und gesetzliche Verantwortung vom VR und GL



3.1
Gesetzliche Grundlagen

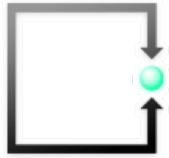


Gesetzliche Verantwortung

Corporate Governance

Corporate Governance (deutsch: Grundsätze der Unternehmensführung) bezeichnet den Ordnungsrahmen für die Leitung und Überwachung von Unternehmen.[1][2] Der Ordnungsrahmen wird maßgeblich durch Gesetzgeber und Eigentümer bestimmt. Die konkrete Ausgestaltung obliegt dem Aufsichts- bzw. Verwaltungsrat und der Unternehmensführung.

Das unternehmensspezifische Corporate Governance-System besteht aus der Gesamtheit relevanter Gesetze, Richtlinien, Kodizes, Absichtserklärungen, Unternehmensleitbild, und Gewohnheit der Unternehmensleitung und -überwachung.



Gesetzliche Verantwortung (2)

**Bundesgesetz
betreffend die Ergänzung
des Schweizerischen Zivilgesetzbuches
(Fünfter Teil: Obligationenrecht)**

vom 30. März 1911 (Stand am 1. Januar 2017)

Art. 716[456]

III. Aufgaben
1. Im Allgemeinen

[1] Der Verwaltungsrat kann in allen Angelegenheiten Beschluss fassen, die nicht nach Gesetz oder Statuten der Generalversammlung zugeteilt sind.

[2] Der Verwaltungsrat führt die Geschäfte der Gesellschaft, soweit er die Geschäftsführung nicht übertragen hat.

Gesetzliche Verantwortung (3)

Art. 716a[457]

2. Unübertragbare Aufgaben

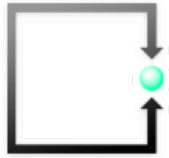
[1] Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes[458] sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

[2] Der Verwaltungsrat kann die Vorbereitung und die Ausführung seiner Beschlüsse oder die Überwachung von Geschäften Ausschüssen oder einzelnen Mitgliedern zuweisen. Er hat für eine angemessene Berichterstattung an seine Mitglieder zu sorgen.

Gesetzliche Verantwortung (4)

- Organisationsverantwortung als unübertragbare und unentziehbare Aufgabe des Verwaltungsrates (Art. 716a Abs. 1 und 2 OR)
- Complianceverantwortung des VR (Art. 716a Abs. 1 OR)
- Unternehmensverantwortung des VR (Art. 716a Abs. 1 OR)
- Verantwortung für Personalauswahl des VR (Art. 716a Abs. 4 OR)
- Führungsverantwortung des VR (Art. 716a Abs. 5 OR)



Gesetzliche Verantwortung (5)

Art. 717[460]

IV. Sorgfalts- und Treuepflicht

[1] Die Mitglieder des Verwaltungsrates sowie Dritte, die mit der Geschäftsführung befasst sind, müssen ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren.

[2] Sie haben die Aktionäre unter gleichen Voraussetzungen gleich zu behandeln.

Gesetzliche Haftung

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

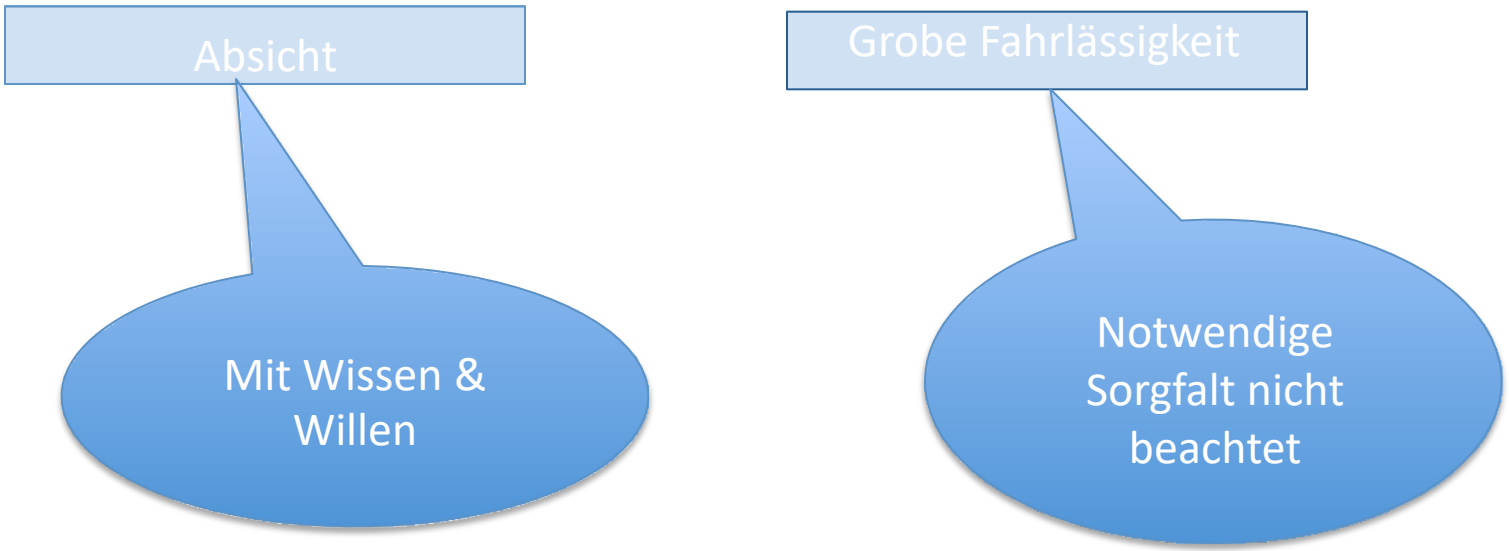
Art. 754[503]

[1] Die Mitglieder des Verwaltungsrates und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als den einzelnen Aktionären und Gesellschaftsgläubigern für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.

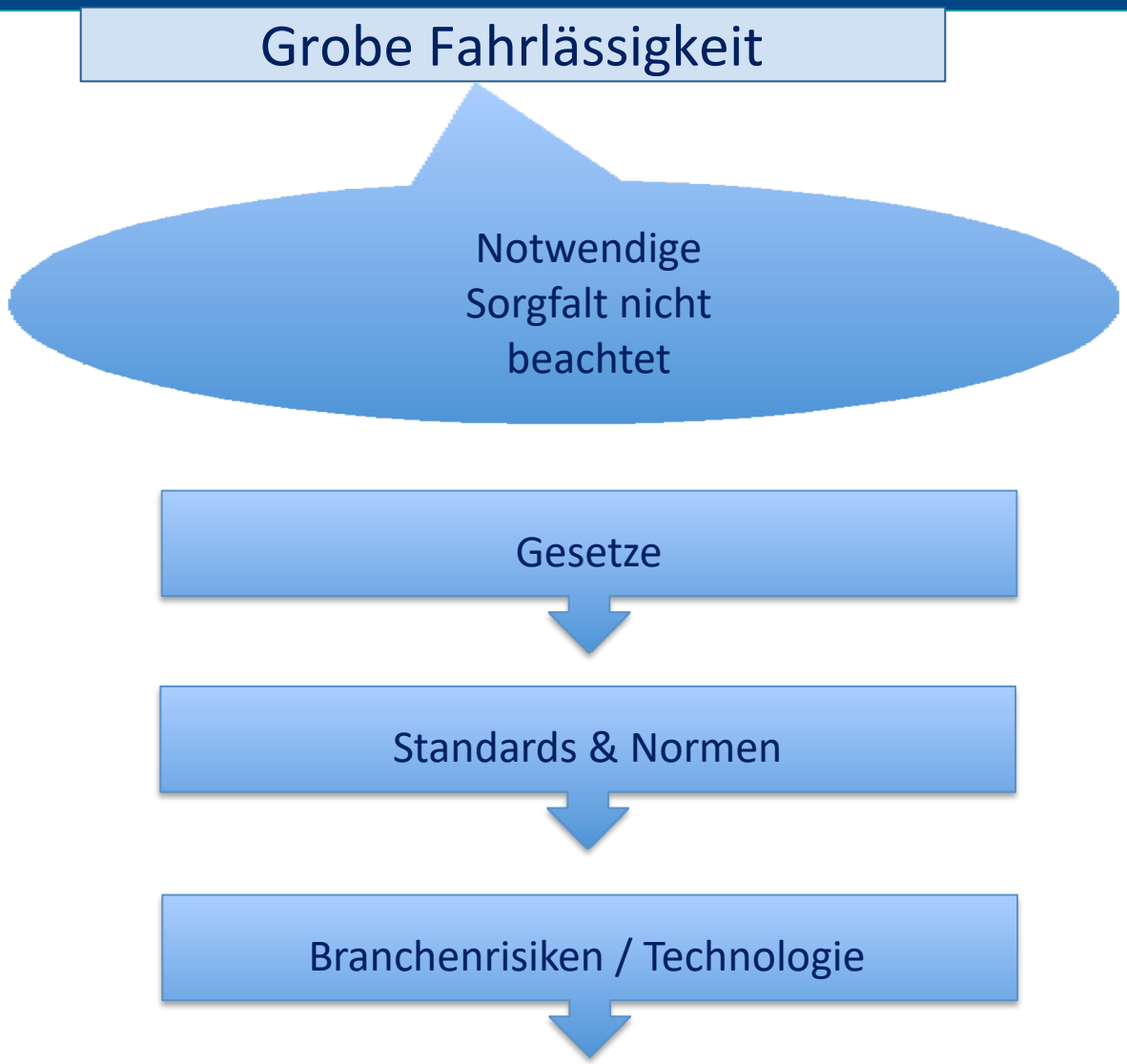
[2] Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

Gesetzliche Haftung (2)

für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen.



Gesetzliche Haftung (3)



Gesetzliche Haftung (4)

**Bundesgesetz
betreffend die Ergänzung
des Schweizerischen Zivilgesetzbuches
(Fünfter Teil: Obligationenrecht)**

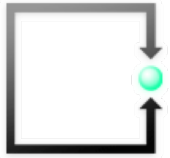
vom 30. März 1911 (Stand am 1. Januar 2016)

III. Haftung für Verwaltung, Geschäftsführung und Liquidation

sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.

Sorgfalt in der Auswahl	=	Evaluieren
Sorgfalt in der Unterrichtung	=	Kommandieren
Sorgfalt in der Überwachung	=	Kontrollieren
Sorgfalt in der Verbesserung	=	Korrigieren

3.2
Softlaw:
Standards, Normen und Richtlinien



Standards, Normen & Richtlinien

Swiss Code of Best Practice for Corporate Governance

https://www.economiesuisse.ch/de/publikationen/swiss-code-best-practice-corporate-governance

economiesuisse

Umgang mit Risiken und Compliance, internes Kontrollsystem

20

Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes Risikomanagement und ein internes Kontrollsystem. Das Risikomanagement bezieht sich auf finanzielle, operationelle und reputationsmässige Risiken.

- Das interne Kontrollsystem ist der Grösse, der Komplexität und dem Risikoprofil der Gesellschaft anzupassen.
- Das interne Kontrollsystem deckt, je nach den Besonderheiten der Gesellschaft, auch das Risikomanagement ab.
- Die Gesellschaft richtet eine interne Revision ein. Diese erstattet dem Prüfungsausschuss («Audit Committee») und gegebenenfalls dem Präsidenten des Verwaltungsrats Bericht.

Standards, Normen & Richtlinien (2)

economiesuisse

21

Der Verwaltungsrat trifft Massnahmen zur Einhaltung der anwendbaren Normen (Compliance).

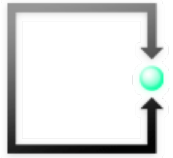
- Der Verwaltungsrat ordnet die Funktion der Compliance nach den Besonderheiten des Unternehmens und erlässt geeignete Verhaltensrichtlinien.
- Er orientiert sich dabei an anerkannten Best Practice-Regeln.[3]
- Der Verwaltungsrat gibt sich mindestens einmal jährlich darüber Rechenschaft, ob die für ihn und das Unternehmen anwendbaren Compliance-Grundsätze hinreichend bekannt sind und ihnen dauernd nachgelebt wird.

Standards, Normen & Richtlinien (3)

Internationale Standards:

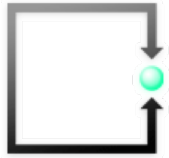
ISO-Normen	**ISO 9001** **ISO 27001 IT-Security** **ISO 20000 Service Mgmt** **ISO 15489 Records Mgmt** **ISO 14721 Archival Mgmt**
Branchen-Standard	**Deutschland:** **Bundesamt für Sicherheit in der Informations-technik** https://www.bsi.bund.de **Das Standard-Datenschutzmodell vom 10.11.2016 (Konferenz Datenschutzbehörden DE)**

4
Die wichtigsten Aspekte für Unternehmen

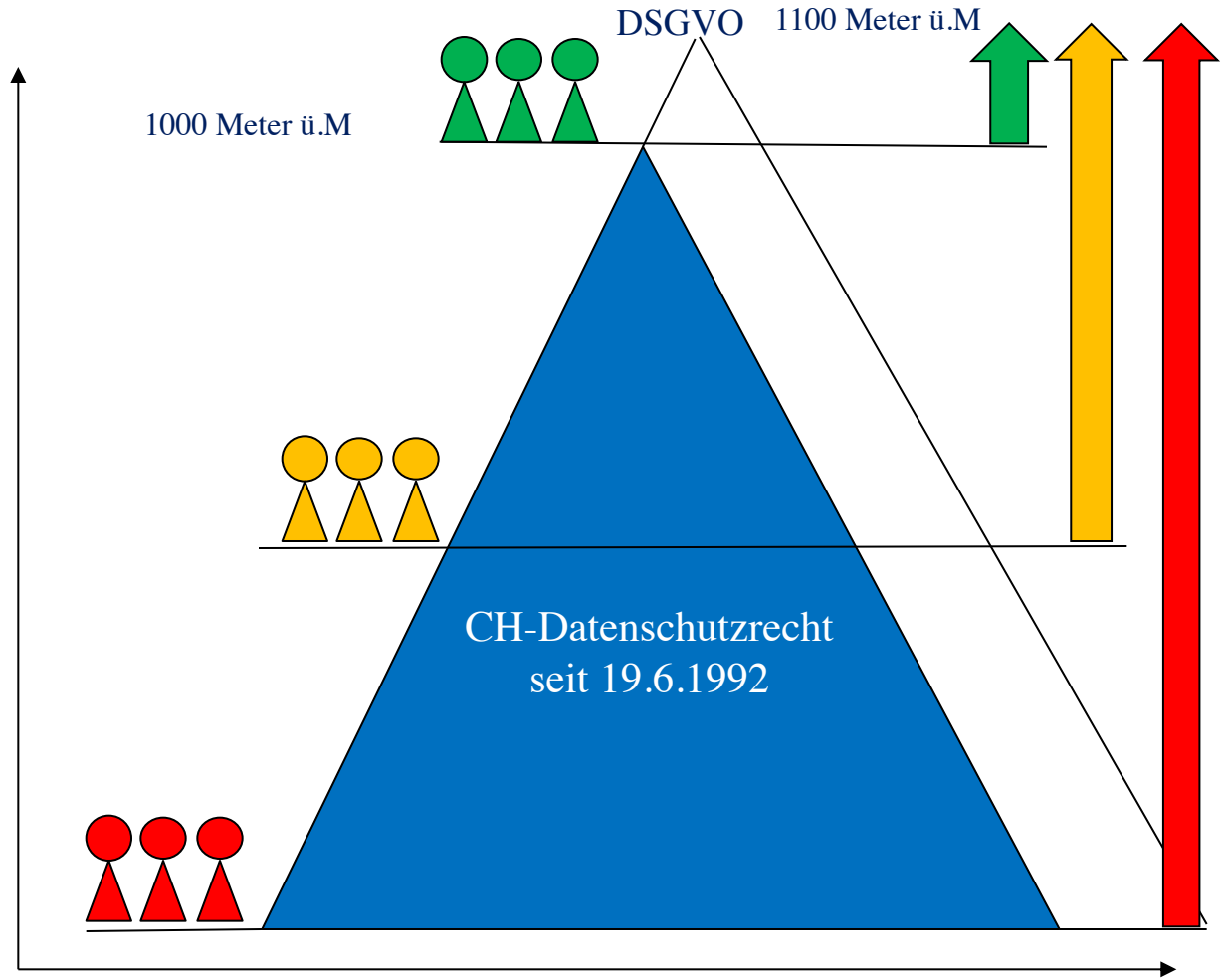


Die 5 wichtigsten Sachen für Unternehmen

Personenbezogene Daten (+ Profiling-Daten)	evaluieren
Dokumentationspflichten	erfüllen
Betroffenenrechte	sicherstellen
Organisatorische Massnahmen im Innenverhältnis & im Aussenverhältnis	ergreifen
Technische Massnahmen	ergreifen

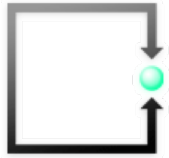


Distanzen zur Erfüllung

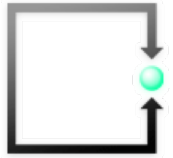


Der effektive Wandel

- Vieles ist gleich geblieben
- Einiges wurde umbenannt
- Einiges wurde intensiviert
- Einiges hat sich verändert



5
Die (neuen) Begriffe



Die (neuen) Begriffe

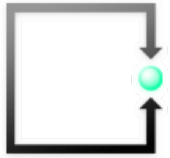
Personenbezogene Daten

Betroffene

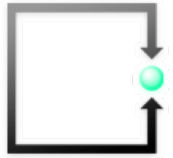
Verantwortlicher

Auftragsverarbeiter

Ausdrückliche Einwilligung



Personenbezogene Daten



Sachlicher Geltungsbereich

Art. 2 § 1 und Art. 4 DSGVO

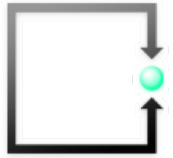
- DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung **personenbezogener Daten** (nur noch dieser Begriff) sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden.

- Gilt auch für **Profiling-Daten**
  Erstellung, Aktualisierung und Verwendung von Profilen durch Sammlung von (auch im Internet gewonnener) Daten, sowie deren anschließende Analyse und Auswertung, zum Zwecke der Identifikation und Überwachung von Personen, auch zur Optimierung und Vorhersage des (Direkt)marketings oder zum Zwecke der Wahl-, Verhaltens- und Meinungsbeeinflussung.

- Gilt für jede Bearbeitung personenbezogener Daten, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen

- Gilt für **alle natürlichen Personen** oder **juristische Personen** des **öffentlichen Rechts** oder des **privaten Rechts**, die Daten verarbeiten.

Betroffene



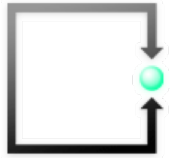
Betroffene

Art. 4 § 1 DSGVO

- **Betroffene** sind identifizierbare oder identifizierte natürliche Personen,

- welche **direkt** oder **indirekt**, insbesondere mittels Zuordnung zu
  - einer Kennung wie einem Namen,
  - einer Kennnummer,
  - zu Standortdaten,
  - zu einer Online-Kennung oder
  - zu einem oder mehreren besonderen Merkmalen, die Ausdruck der
    - physischen,
    - physiologischen,
    - genetischen,
    - psychischen,
    - wirtschaftlichen,
    - kulturellen oder
    - sozialen Identität

  dieser natürlichen Person sind.



Betroffene (2)

Wer sind Betroffene

- **Mitarbeiter**
- **Kunden**
- **Lieferanten**

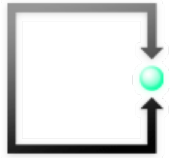
Personenbezogene Daten

Gesetzeskonforme (ordentliche) Behandlung

Betroffenenrechte

Vgl. Ziffer 8 Präsentation

Verantwortlicher



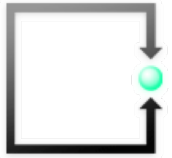
Verantwortlicher

Art. 4 § 7 DSGVO

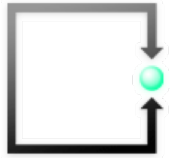
- **Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,

- die allein oder gemeinsam mit anderen
- über die Zwecke und Mittel der Verarbeitung
- von personenbezogenen Daten
- entscheidet.

Es ist der Dateninhaber, der personenbezogene Daten allein oder gemeinsam mit anderen verarbeitet.



Auftragsverarbeiter



Auftragsverarbeiter

Art. 4 § 8 DSGVO

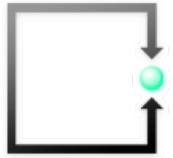
- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,

- welche die personenbezogenen Daten
- im Auftrag des Verantwortlichen
- Verarbeitet.

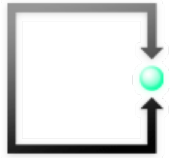
Es ist der Dritte, der im Auftrag des Verantwortlichen personenbezogene Daten wo auch immer verarbeitet.

Er kommt in eine neue umfassende Mitverantwortung im Rahmen des Datenschutzes

Der **Verantwortliche** muss den **Auftragsverarbeiter** kontrollieren (**Joint Controllingship**; vgl. Beilage 11)



Ausdrückliche Einwilligung



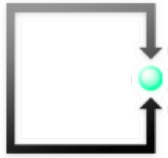
Ausdrückliche Einwilligung

Art. 4 § 11 DSGVO

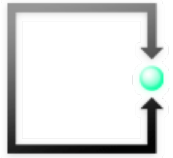
- **Ausdrückliche Einwilligung** ist

- jede freiwillig für den bestimmten Fall,
- in informierter Weise und
- unmissverständlich abgegebene Willensbekundung
- in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung,
- mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

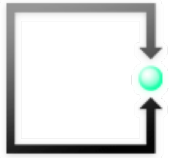
- Die ausdrückliche Einwilligung ist **jederzeit widerrufbar** (Betroffenenrechte –> eingeschränkte Nutzung –> Anspruch auf Löschung meiner gespeicherten und verarbeiteten personenbezogenen Daten).



6
Örtlicher und sachlicher Anwendungsbereich der DSGVO



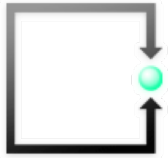
6.1
Sachlicher Anwendungsbereich der DSGVO



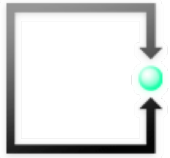
Sachlicher Geltungsbereich

- Jedes **Verarbeiten** von personenbezogenen Daten durch Verantwortliche mit oder ohne Auftragsverarbeiter auf der Basis einer gesetzlichen Grundlage oder mit ausdrücklicher Einwilligung des Betroffenen.

- **Verarbeiten** (Art. 4 § 2 DSGVO)
- Jeder
  - mit oder ohne Hilfe automatisierter Verfahren
  - ausgeführte Vorgang oder jede solche Vorgangsreihe
  - im Zusammenhang mit personenbezogenen Daten wie
    - das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, die Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.



6.2
Räumlicher Anwendungsbereich der DSGVO



Räumlicher Geltungsbereich

Art. 3 DSGVO

- Erweiterter Anwendungsbereich gegenüber RL 95/46/EG
- Extraterritoriale Anwendung (EuGH 2014: Google Spanien)

- Kriterium **Niederlassung**
  Wenn der Verantwortliche seine **Niederlassung in der EU** hat, unabhängig davon wo die Datenbearbeitung stattfindet. (§ 3 Abs. 1 DSGVO)

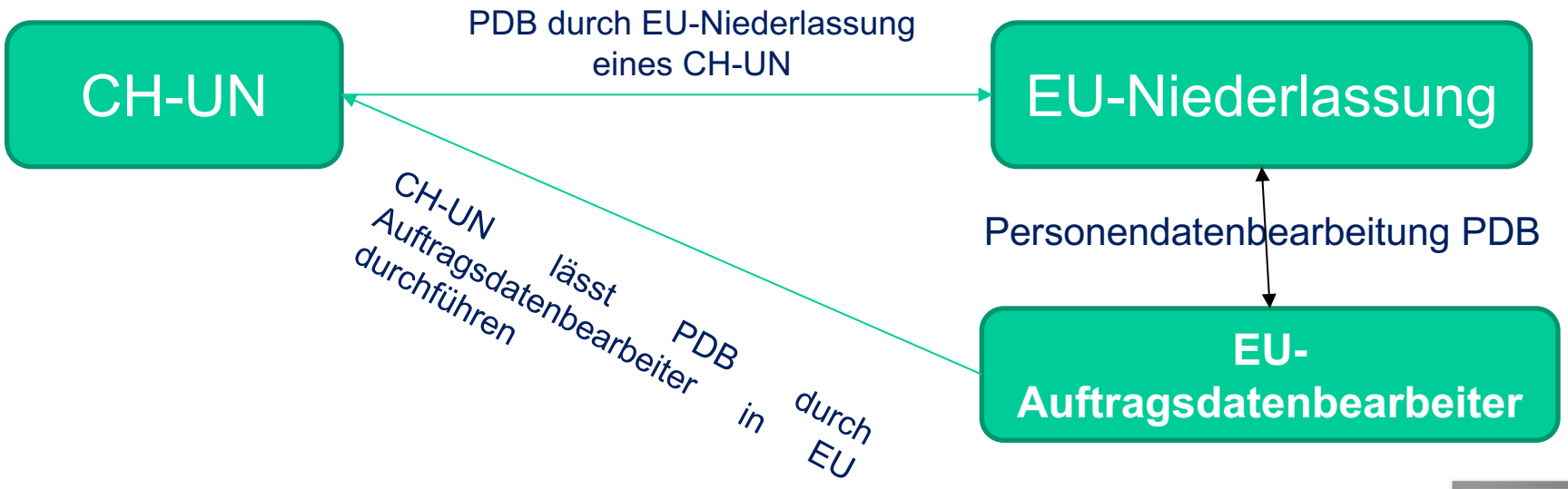
- Kriterium **Zielmarkt**
  Wohnort der von Datenbearbeitung **betroffenen Person in der EU** (§ 3 Abs. 2 DSGVO)
  Die Niederlassung des Verantwortlichen ist ausserhalb EU, aber die Datenbearbeitung betrifft Waren oder Dienstleistungen, die für Personen in der EU bestimmt sind oder die Bearbeitung betrifft Beobachtung des Verhaltens einer betroffenen Personen, soweit deren Verhalten in der Union erfolgt (Achtung Cookieseinsatz).

Extraterritoriale Wirkung der DSGVO

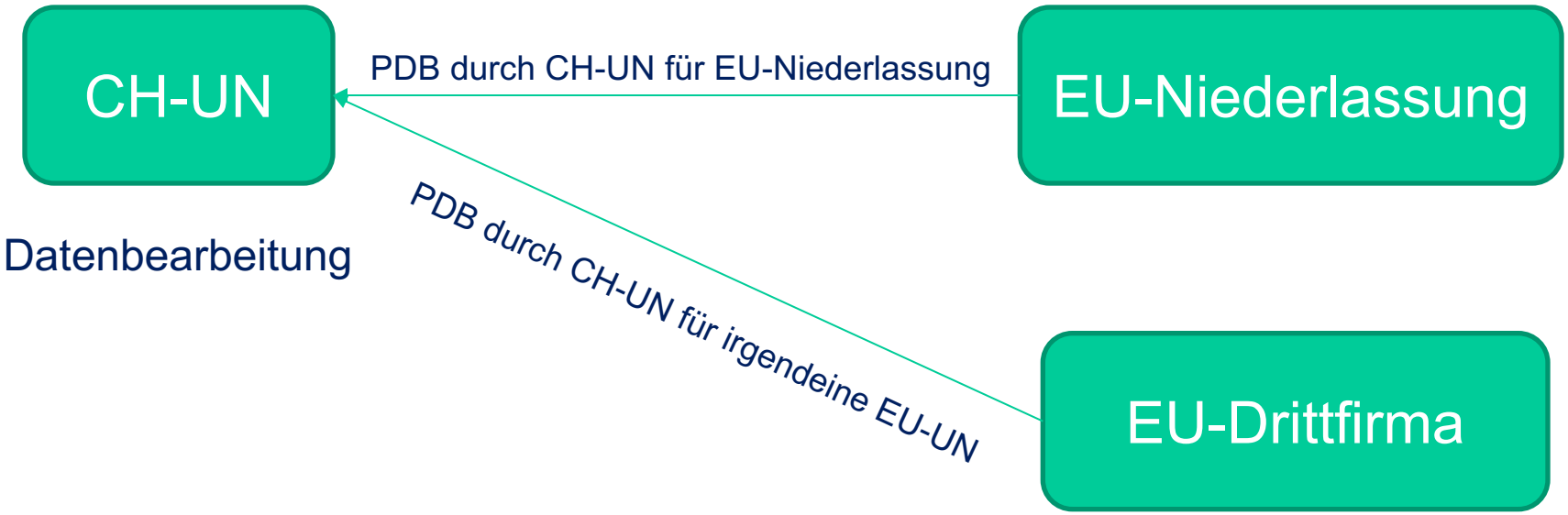
Artikel 3

Räumlicher Anwendungsbereich

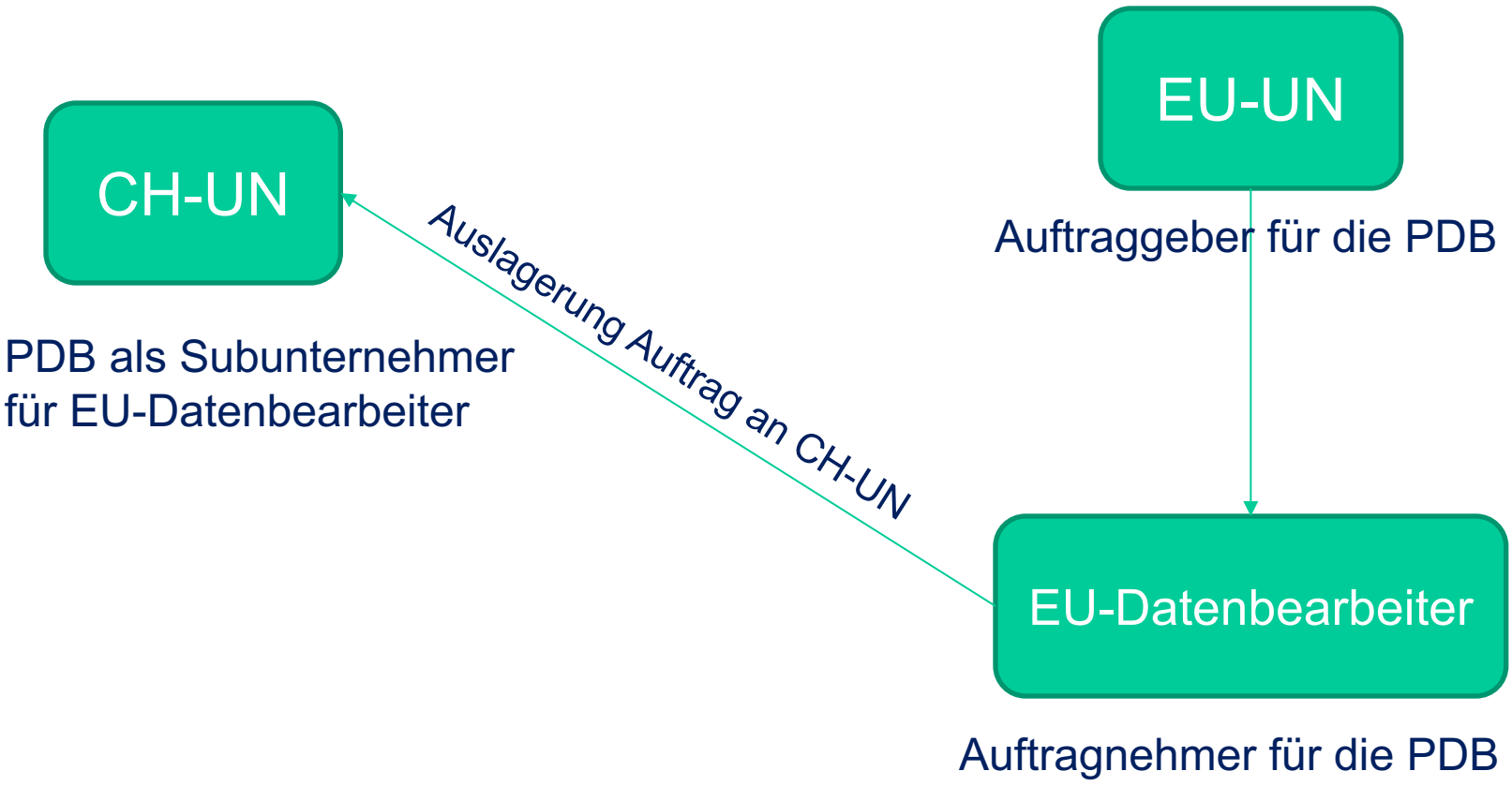
(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.



Extraterritoriale Wirkung der DSGVO



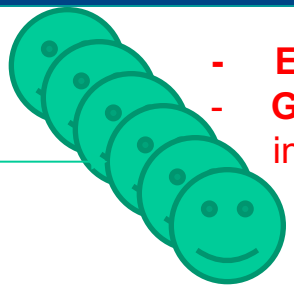
Extraterritoriale Wirkung der DSGVO



Marktortprinzip in Onlinehandel

CH-UN Onlineshop

Angebot von Waren oder Dienstleistungen (auch) an EU-Konsumenten



- **EU-Konsumentenrecht**
- **Gerichtsstand** am Wohnsitz in EU-Land

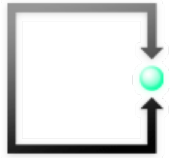
Eher unproblematisch

- Zugänglichkeit einer E-Mailadresse
- Verwendung der Sprache des Ziellandes

Problematisch (insbesondere in Kombination)

- Sprache oder Währung in Verbindung mit Möglichkeit zur Bestellung von Waren in dieser Sprache oder Währung
- Reklame mit Kundenfeedback von EU-Konsumenten
- Gezielte Werbung an Kunden nin bestimmten EU-Staaten (Ferienangebote an Italiener)
- Angabe von Versandkosten in einzelne EU-Länder
- Lieferhinweise für EU-Lieferungen
- Vorgaben für Abwicklung von Bestellungen in EU-Länder
- Angabe einer Bankverbindung in EU-Land
- Hinweise auf Rechtsvorschriften von EU-Ländern
- Betreiben einer Webseite mit einer länderspezifischen Top-Level-Domain

7
Das Standard-Datenschutzmodell SDM



SDM - Standard Datenschutzmodell

Das Standard-Datenschutzmodell

Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele

Beilage 04

V.1.0 – Erprobungsfassung

von der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 9. und 10. November 2016 in Kühlungsborn einstimmig zustimmend zur Kenntnis genommen (Enthaltung durch Freistaat Bayern)

https://www.datenschutz-mv.de/datenschutz/datenschutzmodell (vgl. auch Beilage 04)

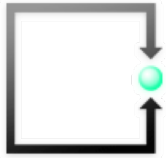
SDM - Standard Datenschutzmodell (2)

Standard-Datenschutzmodell

Die 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat am 9. November 2016 die Version 1.0 des Standard-Datenschutzmodells (SDM) zustimmend zur Kenntnis genommen (einstimmig bei Enthaltung Bayerns).

Das SDM richtet sich einerseits an die Stellen, die für die Verarbeitung personenbezogener Daten verantwortlich sind. Diese können mit dem SDM die erforderlichen Funktionen und Schutzmaßnahmen systematisch planen, umsetzen und kontinuierlich überwachen. Das Modell richtet sich zudem an die Datenschutzbehörden, um mit einer einheitlichen Systematik zu einem transparenten, nachvollziehbaren, belastbaren Gesamturteil über ein Verfahren und dessen Komponenten zu gelangen. Das SDM soll einen wesentlichen Beitrag leisten, um einen an Grundrechten orientierten Datenschutz durchzusetzen.

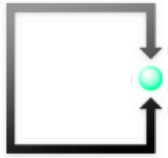
Der Maßnahmenkatalog zum SDM befindet sich noch in der Erarbeitungsphase. Die einzelnen Bausteine des Katalogs werden sukzessive veröffentlicht und zur Anwendung freigegeben.



DSGVO-Grundsatzvorschriften

Art. 5 DSGVO
Art. 12 DSGVO
Art. 25 DSGVO
Art. 32 DSGVO

- Die Verarbeitung personenbezogener Daten (inkl. Profiling-Daten) hat sich am Recht auf **informationelle Selbstbestimmung** auszurichten (BVerfG Urteil vom 15.12.1983, 1 BvR 209/83, „Volkszählungsurteil“).
- **Personendaten sind zu schützen.**
- **Verarbeitung** muss **sicher** sein.
- **Geeignete organisatorische und technische Massnahmen** ergreifen.
- um dem Risiko bei der Verarbeitung ein angemessenes Schutzniveau zu gewährleisten.
- Verfahren **zur regelmässigen Überprüfung**, **Bewertung** und **Evaluierung** der **Wirksamkeit der Massnahmen** (Art. 32 Abs. 1 Satz 1 lt. D DSGVO).



SDM – Einleitung (2)

Das SDM bietet geeignete Mechanismen, um diese rechtlichen Anforderungen der DSGVO in technische und organisatorische Massnahmen zu überführen.

Gewährleistungsziele

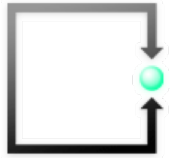
- Alle Anforderungen des Gesetzgebers (DSGVO) werden aufgelistet
- Alle Gewährleistungsziele sind gesetzlich abgedeckt
- Alle datenschutzrechtlichen Vorschriften können den Gewährleistungs-zielen zugeordnet werden („**Mapping**“)
- Sie sollen normgerechte Verarbeitung von Personendaten sicherstellen
- Fokus: Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten
- **Gewährleistungsziele** müssen in jedem Fall **vor jeder Verarbeitung** von personenbezogenen Daten **geprüft** werden
- Der **Verantwortliche** muss die Erfüllung dieser Gewährleistungsziele **nachweisen** **(neuer Grundsatz in DSGVO)** können

Massnahmen-Katalog

Katalog
von technischen und organisatorischen **Massnahmen**

- Beinhaltet alle generischen Massnahmen zur Umsetzung der Gewährleistungs-ziele
- Je Gewährleistungsziel -> Massnahmenmöglichkeiten (Katalog)
- Datenschutz- Risikobeurteilung -> Schutzbedarfskategorien („normal“, „hoch“, „sehr hoch“)
- Datenschutz-Folgeabschätzung, wenn besondere Risiken im Rahmen der Verarbeitung personenbezogener Daten bestehen
- Der **Verantwortliche** muss die Erfüllung dieser **Massnahmen nachweisen (neuer Grundsatz in DSGVO)** können

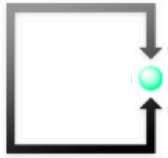
7a
Das Standard-Datenschutzmodell
Die Gewährleistungsziele



Übersicht Gewährleistungsziele

Gewährleistungsziele

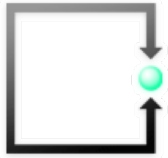
1. Datenminimierung
2. Verfügbarkeit
3. Integrität
4. Vertraulichkeit
5. Nichtverkettung
6. Transparenz
7. Intervenierbarkeit
8. Authentizität
9. Revisionsfähigkeit



Gewährleistungsziele

Datenminimierung (Art. 5 c DSGVO)

- **Datenstrom auf Wesentliches und auf ein notwendiges Mass beschränken**
  Nicht mehr personenbezogene Daten erheben, verarbeiten und nutzen, als für das Erreichen des Verarbeitungszweckes erforderlich
- Proaktives Element datenschutzfreundlicher Technikgestaltung (Privacy by default - Privacy by design)
- Gilt **über den ganzen Lebenszyklus** der Daten von der **Erhebung** über **Verarbeitung** und **Nutzung** bis zur **Lösung** oder **vollständigen Anonymisierung**



Gewährleistungsziele

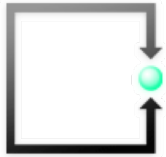
Verfügbarkeit (Art. 5 Abs. 1 e) und 32 Abs. 1 b) und c) DSGVO)

- **Personenbezogene Daten müssen zur Verfügung stehen und ordnungsgemäss im vorgesehenen Prozess verwendet werden**
- Gewährleistet die Verfügbarkeit der Daten zum jeweiligen Zweck, solange dieser noch besteht
- **Kommt zum Tragen bei den Informations- und Auskunftspflichten** (Art. 13 und 15 DSGVO)
- Für das **Recht auf Datenübertragbarkeit** (Art. 20 DSGVO) ist die Verfügbarkeit zudem Grundvoraussetzung

Gewährleistungsziele

Integrität (Art. 5 Abs. 1 f) und 32 Abs. 1 b) DSGVO)

- **Personenbezogene Daten dürfen nicht unbefugt verändert oder entfernt werden**
- Personenbezogene Daten müssen unversehrt, vollständig, richtig und aktuell bleiben
- Abweichungen von diesen Anforderungen müssen ausgeschlossen oder mindestens feststellbar (Logdateien) sein



Gewährleistungsziele

Vertraulichkeit **(Art. 5 Abs. 1 f), 32 Abs. 1 b), 28 Abs. 3 b) und 38 Abs. 5 DSGVO)**

- **Schutz vor unbefugter und unrechtmässiger Verarbeitung.**
- Jede Datenverarbeitung ohne Rechtsgrundlage (Gesetzliche Ermächtigung oder ausdrückliche Einwilligung) ist eine Verletzung der Vertraulichkeit
- Zugriff auf personenbezogene Daten muss über technische und organisatorische Massnahmen mittels (**rollenbasierten**) **Berechtigungs-konzepten** und/oder **Metadaten** (Klassifizierungen) sichergestellt sein
- Insbesondere zu beachten: **Geheimhaltungspflicht des Auftragsdaten-verarbeiters i**n Art. 28 Abs. 3 b) DSGVO

Gewährleistungsziele

Nichtverkettung (Art. 5 Abs. 1 c) und 7 Abs. 4 DSGVO)

- **Personenbezogene Daten dürfen nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden**
- **Verarbeitungsbefugnisse** können der **Geschäftszweck** oder die **ausdrückliche Einwilligung** mit **umfassender Offenlegung des Verwendungszweckes**
- **Kombination mit öffentlich zugänglichen Daten** (Big Data) ist nur für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke **in DSGVO abgedeckt.**
- Typische Massnahme zur Nichtverkettung ist die „Pseudonymisierung“ (vgl. Art. 40 Abs. 2 d) DSGVO)

Gewährleistungsziele

Transparenz (Art. 5 Abs. 1 a) DSGVO und zahlreiche weitere Regeln)

- Verantwortliche, Betroffene, Betreiber von Systemen und Kontroll-instanzen können erkennen,
  - welche Daten
  - für welche Zwecke
  - in welchem Verfahren erhoben und verarbeitet werden
  - welche Systeme und Prozesse dafür genutzt werden
  - wohin die Daten
  - zu welchem Zweck fliessen und
  - wer die rechtliche Verantwortung für die Daten und System in den verschiedenen Phasen einer Datenverarbeitung besitzt
- Absolute Voraussetzung für eine gültige ausdrückliche Einwilligung des Betroffenen

Gewährleistungsziele

Intervenierbarkeit (Art. 16 und 17 DSGVO)

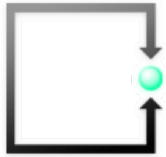
- **Den Betroffenen müssen die ihnen zustehende Rechte auf**
  - **Benachrichtigung** (z.B. Datenbearbeitung oder Data Breaching)
  - **Auskunft**
  - **Berichtigung**
  - **Sperrung**
  - **Löschung**

  jederzeit wirksam gewährt werden.
- Verantwortliche müssen **jederzeit** in der Lage sein, **in die Datenverarbeitung** vom Erhebung bis zum Löschen der Daten **einzugreifen**

Gewährleistungsziele

Authentizität (abgeleitetes Gewährleistungsziel aus obigen)

- **Personenbezogene Daten müssen ihrem Ursprung gesichert zugeordnet werden können**
- Verantwortliche müssen **jederzeit** in der Lage sein, **die Datenquellen, Anlass und Zweck der Übermittlung, Beschaffung, Beschaffungszweck nachzuweisen**

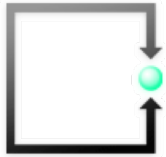


Gewährleistungsziele

Revisionsfähigkeit (abgeleitetes Gewährleistungsziel aus obigen)

- **Es muss festgestellt werden können,**
  - **wer**
  - **wann**
  - **welche personenbezogenen Daten**
  - **in welcher Weise**

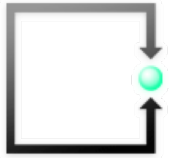
  verarbeitet hat
- Verantwortliche müssen **jederzeit** in der Lage sein, **die Verarbeitung, Nutzung, die blosse Kenntnisnahme, Veränderung, Ergänzung, Berichtigung, Sperrung, Löschung nachzuweisen zu können**



Übersicht Gewährleistungsziele (11)

Zuordnung der **Artikel der DSGVO** zu den **Gewährleistungszielen**

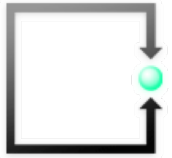
Datenminimierung	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettung	Transparenz	Intervenier-barkeit
5 Abs. 1 lit c 5 Abs. 1 lit e 25 32	5 Abs. 1 lit e 13 15 20 25 32	5 Abs. 1 lit f 25 32 33	5 Abs. 1 lit f 25 28 Abs. 3 lit b 29 32	5 Abs. 1 lit c 5 Abs. 1 lit e 17 22 25 40 Abs. 2 lit d	5 Abs. 1 lit a 13 14 15 19 25 30 32 33 40 42	5 Abs. 1 lit d 5 Abs. 1 lit f 13 Abs. 2 lit c 14 Abs. 2 lit d 15 Abs. 1 lit e 16 17 18 20 21 25 32



Übersicht Gewährleistungsziele (21)

Zuordnung der **Erwägungsgründe der DSGVO** zu den **Gewährleistungszielen**

Datenminimierung	Verfügbarkeit	Integrität	Vertraulichkeit	Nichtverkettung	Transparenz	Intervenier-barkeit
28 29 30 39 78 156	49 78 83	39 49 78 83	39 49 78 83	31 32 33 39 50 53 71 78	32 39 42 58 60 61 63 74 78 84 85 86 87 90 91 100	39 59 65 66 67 68 69 70 78



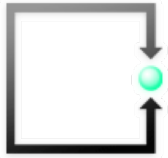
7b
Das Standard-Datenschutzmodell
Die generischen Massnahmen zur Umsetzung der Gewährleistungsziele

Übersicht generische Massnahmen

Katalog
von technischen und organisatorischen **Massnahmen**

Datenminimierung kann erreicht werden durch:

- Reduzierung von erfassten Attributen der betroffenen Personen
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen
- Implementierung automatisierter Sperr- oder Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren



Übersicht generische Massnahmen (2)

Katalog
von technischen und organisatorischen **Massnahmen**

Verfügbarkeit kann erreicht werden durch:

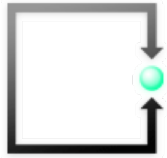
- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien
- Schutz vor äusseren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt)
- Dokumentation der Syntax der Daten
- Redundanz von Hard- und Software sowie Infrastrukturen
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Vertretungsregelungen für abwesende Mitarbeitende

Übersicht generische Massnahmen (3)

Katalog
von technischen und organisatorischen **Massnahmen**

Integrität kann erreicht werden durch:

- Einschränkung von Schreib- und Änderungsrechten
- Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäss eines Kryptokonzeptes
- Dokumentierte Zuweisung von Berechtigungen und Rollen
- Prozesse zur Aufrechterhaltung der Aktualität der Daten
- Festlegung des Sollverhaltens von Prozessen und regelmässige Durchführung von Tests zur Feststellung und Dokumenation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmässiges Durchführen von Testes zur Feststellbarkeit der Ist-Zuständige von Prozessen



Übersicht generische Massnahmen (4)

Katalog
von technischen und organisatorischen **Massnahmen**

Vertraulichkeit kann erreicht werden durch:

- Festlegung eines Rechte- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle
- Implementierung eines sicheren Authentisierungsverfahrens
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsgeprüft) und formal zugelassen sind sowie keine Interessenkonflikte bei der Ausübung aufweisen
- Verschlüsselung von gespeicherten oder transferierten Daten
- Schutz vor äusseren Einflüssen
- Speziell ausgestaltete Umgebungen (Räume, Gebäude)

Übersicht generische Massnahmen (5)

Katalog
von technischen und organisatorischen **Massnahmen**

Nichtverkettung kann erreicht werden durch:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- Programmtechnische Unterlassung bzw. Schliessung von Schnittstellen in Verfahren und Verfahrenskomponenten
- Trennung nach Organisations-/Abteilungsgrenzen (Zonierungen)
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten,
- Geregelte Zweckänderungsverfahren

Übersicht generische Massnahmen (6)

Katalog
von technischen und organisatorischen **Massnahmen**

Transparenz kann erreicht werden durch:

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren
- Dokumentation der Verträge mit Mitarbeitenden, externen Dienstleistern, Datenempfängern, Datenversendern
- Dokumentation aller Einwilligungen und Widersprüchen
- Protokollierung von Zugriffen und Änderungen (Logs)
- Nachweis der Quellen von Daten (Authentizität)
- Versionierung
- Dokumentation der Verarbeitungsprozesse

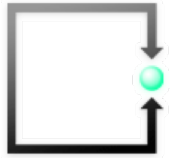
Übersicht generische Massnahmen (7)

Katalog
von technischen und organisatorischen **Massnahmen**

Intervenierbarkeit kann erreicht werden durch:

- Differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten
- Schaffung notwendiger Datenfelder z.B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen
- Dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmassnahmen der IT-Sicherheit und des Datenschutzes
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene
- Prozessbeschreibung für die Einhaltung der Betroffenenrechte

8
DS-Pflichten der UN und Sanktionen



Pflichten der Verantwortlichen (UN)

Übersicht (1)

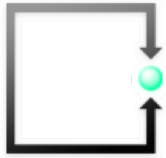
- Rechenschaftspflicht des Verantwortlichen (Art. 5 § 2 DSGVO)
- Einhaltung aller Grundsätze aktiv nachweisen (Art. 5 § 1 DSGVO)
- Umkehr der Beweislast zulasten Verantwortlicher/Bearbeiter
- Wahrscheinlichkeit und Grad der Gefährdung der Rechte der Betroffenen zu Beginn der Bearbeitung beurteilen (Art. 24 DSGVO)
- Privacy by design: Datenschutz bei Produkten und DL muss bereits bei der Planung berücksichtigt werden (Art. 25 DSGVO)
- Privacy by default: Produkte und DL müssen mit daten-schutzfreundlichen Voreinstellung angeboten werden (Art. 25 DSGVO)
- Register der unter seiner Verantwortung ausgeführten Bearbeitungstätigkeiten führen (UN > 250 Beschäftigte) (Art. 30 DSGVO)
- Durchführung einer Datenschutz-Folgeabschätzung, wenn Bearbeitung ein hohes Risiko für die Rechte der Betroffenen zur Folge haben kann (Anforderungen § 35 / 7) (Art. 35 DSGVO)

Pflichten der Verantwortlichen (UN)

Übersicht (2)

- Angemessene organisatorische und technische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO)
  - nach dem Stand der Technik angepasst
  - Regelmässige, nachgewiesene Überprüfung

- Pflicht, der Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten unverzüglich, möglichst innert 72 Stunden zu melden (Art. 33 DSGVO)
  - Meldeinhalt (detailliert in Art. 33 § 3 DSGVO)
  - Dokumentationspflicht (Fakten, Auswirkungen, Abhilfen)
  - Mitteilungspflicht an betroffene Personen (keine Frist) (Art. 34 DSGVO)



Pflichten der Verantwortlichen (UN)

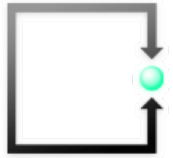
Übersicht (3)

- Benennung eines Datenschutzbeauftragten zwingend für (Art. 37 DSGVO)
  - Alle Behörden und öffentlichen Stellen
  - UN, die Bearbeitungen durchführen, welche eine umfangreiche regelmässige und systematische Überwachung der betroffenen Personen erfordern
  - UN, die sensible Datenbearbeitungsvorgänge (vgl. Folgeabschätzung und Register der Bearbeitungstätigkeiten) durchführen.
  - Nationale Erweiterungen zulässig

- Für **CH-Unternehmen**, die nicht in EU niedergelassen sind: (Art. 27 DSGVO)
  - **Datenschutz-Vertreter in EU-Mitgliedstaat** schriftlich benennen, in welchem die natürlichen Personen ihren Wohnsitz haben, deren personenbezogene Daten oder Profiling-Daten bearbeitet werden
    (Deutschland, Frankreich etc. -> separater Flyer mit Angebot)
    - Ist Ansprechpartner für Aufsichtsbehörden und Betroffene
    - Koordinationsstelle
    - mussRegister aller Kategorien von Tätigkeiten der UN führen
    - Verantwortliche/Bearbeiter bleibt verantwortlich

Beilagen 06, 07, 08, 09, 10

8
DS-Rechte der Betroffenen



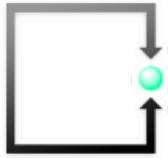
Sanktionen

Aufsichtsbehörden in EU-Ländern

- **Direktes Sanktionierungsrecht** gegenüber UN

- Katalog von Sanktionen (Art. 58 § 2 DSGVO)
  - Mahnung
  - Verwarnung
  - Förmliche Bekanntmachung der UN und des Verstosses
  - Vorübergehende Beschränkung der Datenbearbeitung
  - Dauerhafte Beschränkung der Datenbearbeitung
  - **Geldbussen** von bis zu € 20 Mio oder 4% des weltweiten Jahresumsatzes

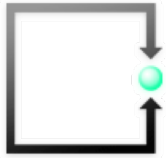
  - Weitergehender Schaden (Schadenersatz und Zinsen) aus einem Gerichtsverfahren bleibt zusätzlich vorbehalten.



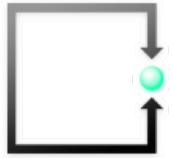
Rechte der Betroffenen

Übersicht

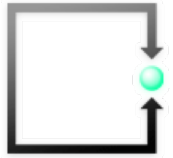
▪ Recht auf Information	(Art. 13/14 DSGVO)
▪ Auskunftsrecht	(Art. 15 DSGVO)
▪ Recht auf Berichtigung	(Art. 16 DSGVO)
▪ Recht auf Löschung («Recht auf Vergessen werden»)	(Art. 17 DSGVO)
▪ Recht auf Einschränkung der Bearbeitung	(Art. 18 DSGVO)
▪ Recht auf Mitteilung	(Art. 19 DSGVO)
▪ Recht auf Datenübertragung	(Art. 20 DSGVO)
▪ Widerspruchsrecht zur Datenbearbeitung	(Art. 21 DSGVO)
▪ Recht auf Verzicht einer automatisierten Entscheidung	(Art. 22 DSGVO)
▪ Recht auf Benachrichtigung über DS-Verletzungen	(Art. 34 DSGVO)
▪ Schutz von Kindern (Altersgrenze zw. 13-16) durch Zustimmung der Inhaber der elterlichen Verantwortung	(Art. 8 DSGVO)



Die neuen Rechte



Recht auf Datenübertragbarkeit



Recht auf Datenübertragbarkeit

Art. 20 DSGVO

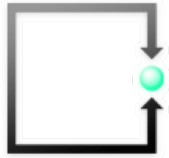
Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten,

- die sie einem **Verantwortlichen bereitgestellt** hat,
- in einem **strukturierten, gängigen und maschinenlesbaren Format** zu erhalten
- und diese **Daten einem anderen Verantwortlichen**
- **ohne Behinderung** durch den Verantwortlichen, dem sie die personenbezogenen Daten bereitgestellt wurden,
- zu **übermitteln**, sofern
    - die Verarbeitung auf einer Einwilligung des Betroffenen beruht und
    - die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

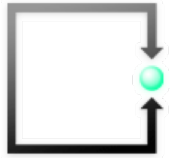
Recht auf direkte Übermittlung vom Verantwortlichen zum anderen Verantwortlichen, soweit dies technisch machbar ist.

Übermittlung darf **Rechte und Freiheiten anderer Personen nicht beeinträchtigen.**

Ausgeschlossen für Verarbeitung, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt.



Widerspruchsrecht



Widerspruchsrecht

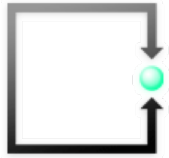
Art. 21 (1, 2 und 6) DSGVO

Die betroffene Person hat das Recht,

- aus Gründen, die sich aus ihrer besonderen Situation ergeben,
- jederzeit **gegen die Verarbeitung** sie betreffender personenbezogener Daten (gilt auch für Profiling-Daten)
- **Widerspruch einzulegen**.
- Ausdrückliche Ausdehnung auf die gesamten Tätigkeiten der Direktwerbung (2)

Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn,

- er kann **zwingende schutzwürdige Gründe** für die Verarbeitung nachweisen,
- welche die **Interessen**, Rechte und Freiheiten der betroffenen Personen **überwiegen**
- oder die Verarbeitung dient der **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** (6)



Widerspruchsrecht (2)

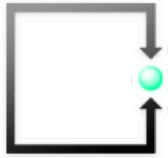
Art. 21 (4) DSGVO

- Die betroffene muss
  - **spätestens zum Zeitpunkt der ersten Kommunikation** mit ihr
  - **ausdrücklich** (wohl mittels Klickfunktion – clickwrapping)
  - auf das genannte Recht auf Widerspruch **hingewiesen** werden;

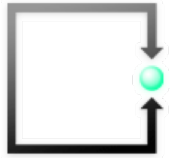
Dieser Hinweis hat
  - in einer **verständlichen** und
  - **von anderen Informationen getrennten Form** (z.B. nicht in AGB einbinden)

zu erfolgen.

Tipp:
Es wird wohl separate Datenschutzbestimmungen brauchen (z.B. für Onlineshops), welche mittels Clickwrapping ausdrücklich angenommen und separat ausserhalb der AGB bereitgestellt werden.



Automatisierte Entscheidungen



Automatisierte Entscheidungen

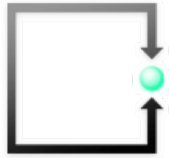
Art. 22 (1) DSGVO

Die betroffene Person hat das Recht,

- nicht einer **ausschliesslich auf einer automatisierten Verarbeitung** – einschliesslich Profiling – **beruhenden Entscheidung** unterworfen zu werden,
- die ihr gegenüber rechtliche Wirkung entfaltet oder
- sie in ähnlicher Weise erheblich beeinträchtigt.

Gilt nicht (2), wenn

- die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages zwischen dem Betroffenen und dem Verantwortlichen erforderlich ist (? automatisierte Bewerberauswertungen ?)
- Rechtsvorschriften der EU oder eines Mitgliedstaates dies zulässig erklären (nationale Öffnungsklauseln)
- Wenn die automatisierte Entscheidung mit ausdrücklicher Einwilligung des Betroffenen erfolgte.



Automatisierte Entscheidungen (2)

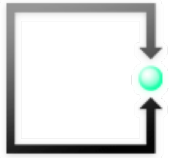
Art. 22 (3) DSGVO

Der Verantwortliche muss **angemessene Massnahmen** ergreifen,

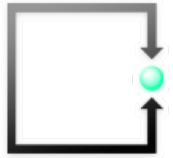
- um die **Rechte und Freiheiten** sowie
- die **berechtigten Interessen** der betroffenen Person **zu wahren**
- das Recht auf **Eingreifen einer natürlichen Person** seitens des Verantwortlichen wahren
- das Recht auf **Darlegung des eigenen Standpunktes** des Betroffenen zulassen
- das Recht auf **Anfechtung der automatisierten Entscheidung** zulassen.

Konsequenzen für Unternehmen:

- Offenlegung automatisierter Entscheidungen
- Anwendung geeigneter (anerkannter) mathematischer oder statistischer Verfahren
- Technische Massnahmen sicherstellen, damit keine Fehler in der automatisierten Entscheidung eintreten
- Keine Algorithmen verwenden, welche Personen aufgrund von Rasse, ethnischer Herkunft, politischer Meinung, Religion oder Weltanschauung, Gewerkschafts-zugehörigkeit, genetischer Anlagen, Gesundheitszustand, sexueller Orientierung etc. diskriminieren
- Dokumentation der Evaluationskriterien sicherstellen
- Entscheidbegründung mit Anfechtungsmöglichkeit



Meldung von Datenschutzverletzungen

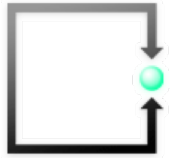


Meldung von Datenschutzverletzungen

Art. 33 und 34 DSGVO

2 neue Benachrichtigungspflichten für Verantwortliche

- **Meldung** von Verletzungen an die **Aufsichtsbehörden** (Art. 33 DSGVO)
- **Benachrichtigung** betroffener Personen (Art. 34 DSGVO)



Meldung von Datenschutzverletzungen (2)

Art. 33 DSGVO
Meldung von Verletzungen an die **Aufsichtsbehörden** (Art. 33 DSGVO)

Im Falle der **Verletzung des Schutzes** personenbezogener Daten meldet der **Verantwortliche**

- **unverzüglich** und **möglichst binnen 72 Stunden**,
- nachdem ihm die Verletzung bekannt wurde,
- diese der **zuständigen Aufsichtsbehörde** (Art. 55 DSGVO), es sei denn, dass
    - die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. (Achtung nur „Risiko“, nicht „erhebliches Risiko“)

- Erfolgt die Meldung nicht binnen 72 Stunden, muss die **Verzögerung** gegenüber der Aufsichtsbehörde **begründet werden**.

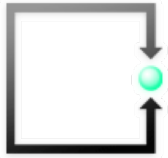
- **Gleiche Informationspflicht** trifft den **Auftragsverarbeiter** gegenüber dem Verantwortlichen

Meldung von Datenschutzverletzungen (3)

Art. 33 (3) DSGVO
Meldung von Verletzungen an die **Aufsichtsbehörden** (Art. 33 DSGVO)

Meldung an Aufsichtsbehörde mit **detaillierten Informationen**:

- **Beschreibung der Art der Verletzung**
- Angaben der **Kategorien der betroffenen Personen** (soweit möglich)
- Ungefähre **Zahl der betroffenen Personen** (soweit möglich)
- **Betroffene Datenkategorien**
- Ungefähre **Zahl der betroffenen Datensätze**
- **Namen und Kontaktdaten des Datenschutzbeauftragten** der Unternehmung oder der **sonstigen Anlaufstelle** (z.B. EU-Datenschutz-Vertreter 27 DSGVO)
- **Beschreibung** der wahrscheinlichen **Folgen der Verletzung**
- **Beschreibung** der vom Verantwortlichen **ergriffenen oder vorges**chlagenen (organisatorischen und/oder technischen) **Massnahmen** zur Behebung der Verletzung
- **Beschreibung** der vom Verantwortlichen **ergriffenen oder vorgeschlagenen** (organisatorischen und/oder technischen) **Massnahmen** zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

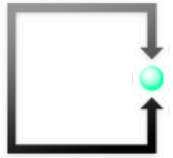


Meldung von Datenschutzverletzungen (4)

Art. 33 (5) DSGVO
Meldung von Verletzungen an die **Aufsichtsbehörden** (Art. 33 DSGVO)

Umfassende Dokumentationspflicht
- Die gesamte Verletzung muss umfassend in Bezug auf **alle massgeblichen Fakten dokumentiert** und
- der **Aufsichtsbehörde zugänglich** gemacht werden.

Benachrichtigung von Datenschutzverletzungen

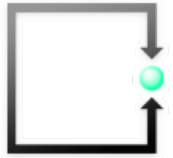


Benachrichtigung von Datenschutzverletzungen

Art. 34 DSGVO
Benachrichtigung von Verletzungen an die **Betroffenen** (Art. 34 DSGVO)

Hat die Verletzung
- voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge,
- so benachrichtigt der Verantwortliche die betroffenen Personen
- unverzüglich von der Verletzung (1).

Die Benachrichtigung muss in **klarer und einfacher Sprache** die **Art der Verletzung beschreiben** (2).

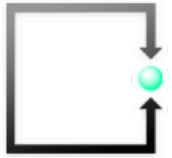


Benachrichtigung von Datenschutzverletzungen (2)

Art. 34 (2) DSGVO
Benachrichtigung von Verletzungen an die **Betroffenen** (Art. 34 DSGVO)

Benachrichtigung enthält zumindest die in **Art. 33 Abs. 3 Bst. b, c und d** genannten **Informationen und Massnahmen**

- **Namen und Kontaktdaten** des **Datenschutzbeauftragten** der Unternehmung oder der **sonstigen Anlaufstelle** (z.B. EU-Datenschutz-Vertreter 27 DSGVO)
- **Beschreibung** der wahrscheinlichen **Folgen der Verletzung**
- **Beschreibung** der vom Verantwortlichen **ergriffenen oder vorgeschlagenen** (organisatorischen und/oder technischen) **Massnahmen** zur Behebung der Verletzung
- Beschreibung der vom Verantwortlichen **ergriffenen oder vorgeschlagenen** (organisatorischen und/oder technischen) **Massnahmen** zur Abmilderung ihrer möglichen nachteiligen Auswirkungen



Benachrichtigung von Datenschutzverletzungen (3)

Art. 34 (3) DSGVO
Benachrichtigung von Verletzungen an die **Betroffenen** (Art. 34 DSGVO)

Benachrichtigung ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Verantwortliche hat **bereits geeignete organisatorische und technische Sicherheitsmassnahmen** getroffen und diese **Vorkehrungen** wurden auf die betroffenen personenbezogenen Daten **bereits angewendet** (z.B. Verschlüsselung);

- Der Verantwortliche bereits durch **Massnahmen** sichergestellt hat, dass **das hohe Risiko** für die Rechte und Freiheiten der Betroffenen aller Wahrscheinlichkeit nach **nicht mehr besteht**;

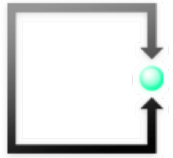
- Diese **individuelle Benachrichtigung** mit einem **unverhältnismässigen Aufwand** verbunden wäre. Stattdessen hat eine **öffentliche Bekanntmachung** oder ähnliche Massnahme zu erfolgen, durch welche die Betroffenen **vergleichbar wirksam informiert** werden.

Benachrichtigung von Datenschutzverletzungen (4)

Art. 34 (4) DSGVO
Benachrichtigung von Verletzungen an die **Betroffenen** (Art. 34 DSGVO)

Hat der Verantwortliche die Betroffenen **nicht bereits benachrichtigt**, kann die **Aufsichtsbehörde** – wenn die Verletzung aus ihrer Sicht wahrscheinlich zu einem hohen Risiko führt – **vom Verantwortlichen verlangen**, diese **Benachrichtigung nachzuholen**

9
Die beigezogenen Datenverarbeiter



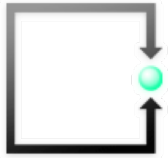
Auftragsverarbeiter

Art. 28 (1) DSGVO
Zusammenarbeit mit Auftragsverarbeiter

Erfolgt eine **Verarbeitung im Auftrag eines Verantwortlichen**, so arbeitet dieser **nur mit Auftragsverarbeitern** zusammen,

- die **hinreichend Garantien** dafür bieten,
- dass **geeignete technische und organisatorische Massnahmen** so durchgeführt werden,
- dass die **Verarbeitung im Einklang mit den Bestimmungen der DSGVO** erfolgt und
- der **Schutz der Rechte der Betroffenen gewährleistet** ist.

Alle Verträge mit Auftragsverarbeitern müssen überprüft und allenfalls angepasst werden



Auftragsverarbeiter (2)

Art. 28 (2 und 3a-h) DSGVO
Zusammenarbeit mit Auftragsverarbeiter

Verantwortlicher braucht (neue) **Verträge** (ausdrücklich in Art. 28 Abs. 3 DSGVO) mit **Auftragsverarbeiter**, welche

- im Detail die aus der Datenschutz-Folgeabschätzung abgeleiteten organisatorischen oder technischen Massnahmen vertraglich überbinden,
- Selber notwendige und aktuelle Massnahmen sicherstellt,
- Gegenstand und Dauer der Verarbeitung regelt (3),
- Art und Zweck der Verarbeitung regelt (3),
- Nur auf dokumentierte Weisung verarbeitet (3a),
- Bearbeitende Personen zur Vertraulichkeit verpflichtet werden (3b),
- Art der personenbezogenen Daten festlegt (3),
- Kategorien betroffener Personen festlegt (3),
- die Rechte und Pflichten des Auftragsverarbeiters dafür statuiert,
- die Service Levels für die Massnahmen definiert,
- die Gewährleistung des Auftragsverarbeiters festlegt,
- die Informationspflichten bei Verletzungen regelt,
- die Haftung des Auftragsverarbeiters definiert,
- ein jederzeitiges Auditrecht (Kontrollrecht bez. Einhaltung der vertraglichen Auflagen) sicherstellt.

Auftragsverarbeiter (3)

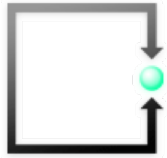
Art. 28 (4) DSGVO
Zusammenarbeit mit Auftragsverarbeiter - Drittbeizug

Zieht der Auftragsverarbeiter seinerseits **Dritte für die Verarbeitung** von personenbezogenen Daten bei, muss er diesem

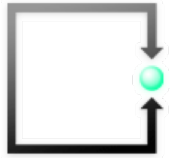
- mittels schriftlichem Vertrag
- dieselben Schutzpflichten auferlegen, die er gemäss Vertrag mit dem Verantwortlichen übernommen hat.

Schriftliche Verträge = kann auch in elektronischem Format (aber rechtsverbindlich) erfolgen

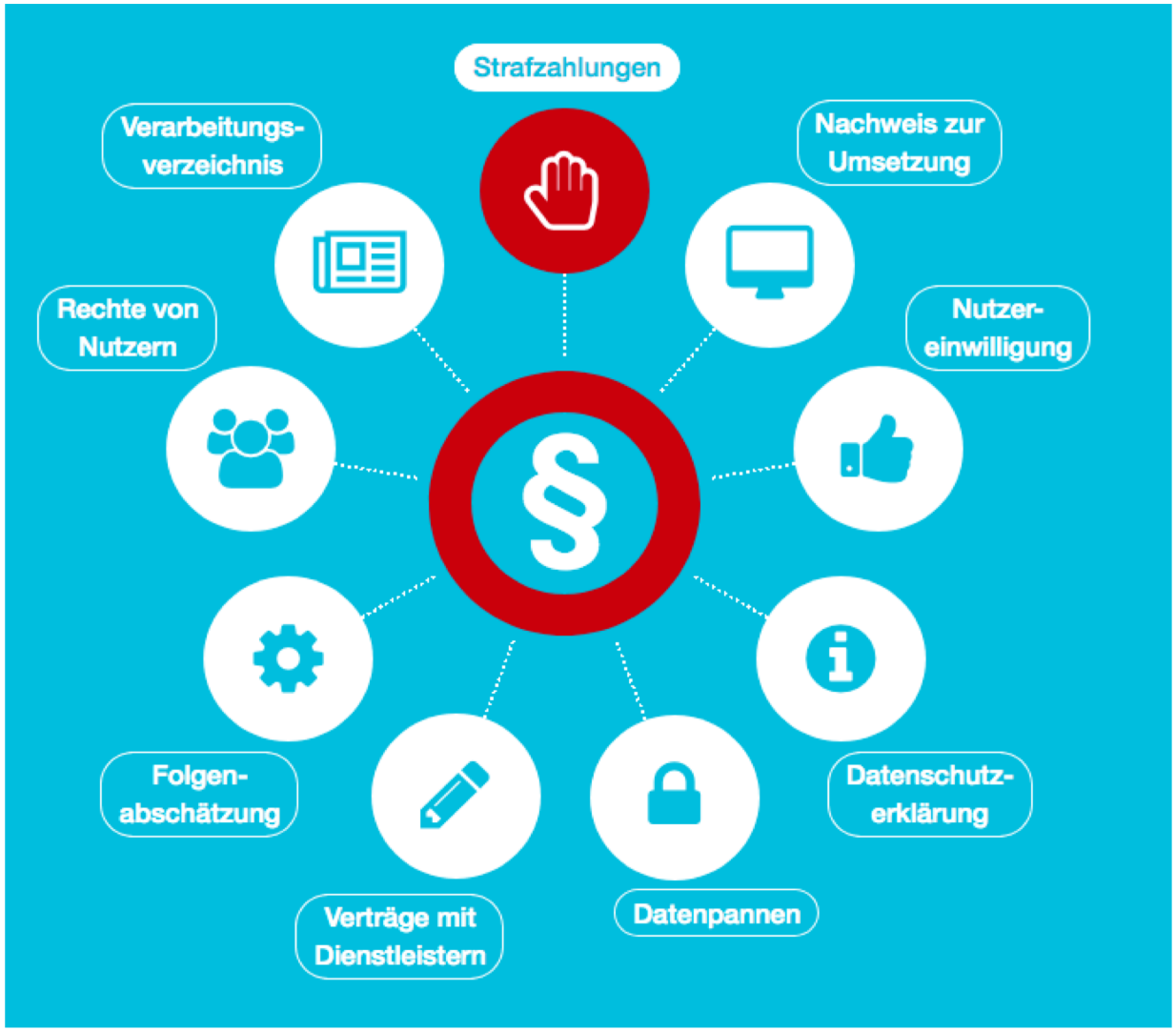
- prüfen ob qualifizierte digitale Signaturen für eigenhändige Unterschriften notwendig sind (Achtung: Behörden- und Unternehmenssiegel nicht keine qualifizierten eigenhändigen Unterschriften)
- Im Handelsregister eingetragene Personen müssen unterzeichnen (Achtung Kollektivunterschriften beachten)



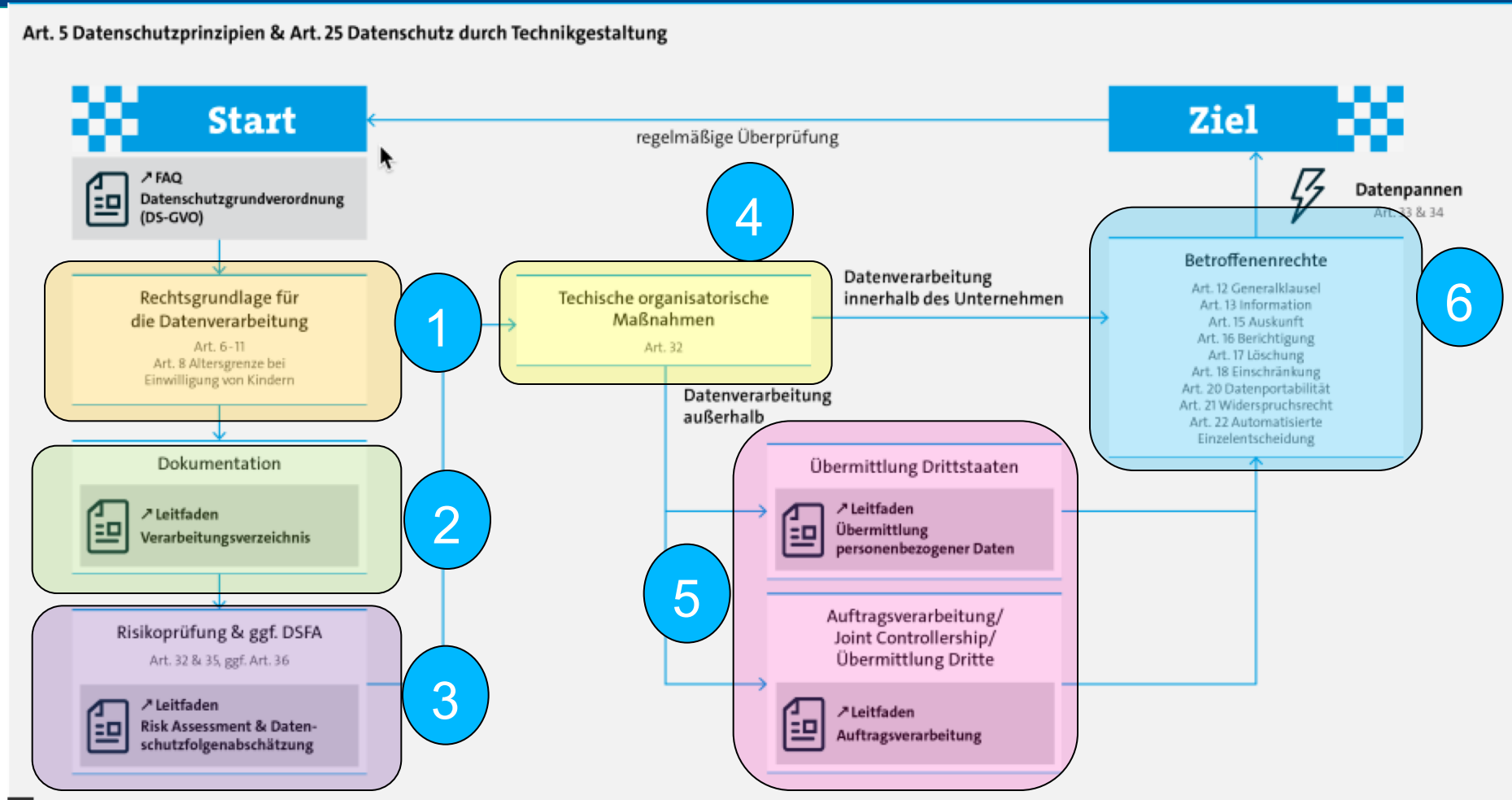
10
Das Projektvorgehen



Die Schwerpunkte



Umsetzung EU- und CH Datenschutz



Quelle: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/Inhaltsseite-2.html

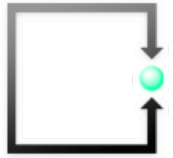
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom)

Unterlagen

1. **Verzeichnis personenbezogenen Daten**
   - Landkarte der personenbezogenen Daten
   - Landkarte der IT-Applikationen
   - Landkarte der Papierakten
   - Übersicht über die Rechtsgrundlage zur Datenverarbeitung

2. **Verzeichnis der Verarbeitungstätigkeiten**

3. **Risikobeurteilung mit Datenschutz-Folgeabschätzung**

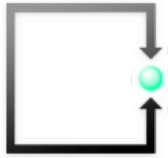


Unterlagen (2)

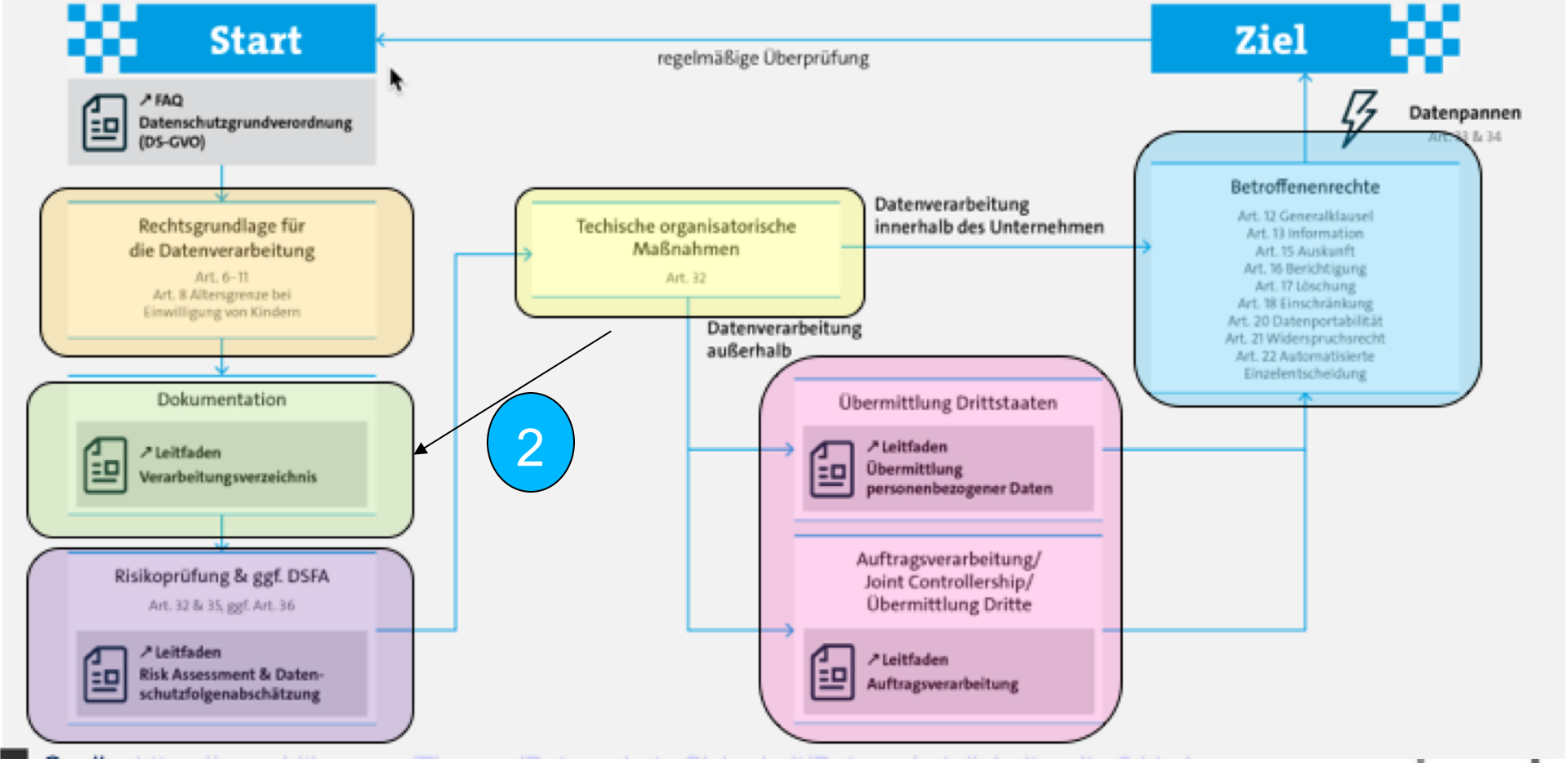
4. Dokumentation organisatorischer und technischer Massnahmen

5. Verträge mit Datenverarbeiter

6. Prozessbeschreibungen bez. aller Betroffenenrechte



Art. 5 Datenschutzprinzipien & Art. 25 Datenschutz durch Technikgestaltung

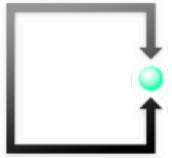


Verzeichnis der Verarbeitungstätigkeiten

Art. 30 (1) DSGVO
Verzeichnis der Verarbeitungstätigkeiten - Verantwortlicher

Jeder Verantwortliche führen ein **Verzeichnis aller Verarbeitung**stätigkeiten. Dieses enthält folgende Angaben:

- **Namen und Kontaktdaten** des **Verantwortlichen**
- **Namen und Kontaktdaten** des **Datenschutzbeauftragten** oder des **EU-Datenschutz-Vertreters des Verantwortlichen**
- **Zwecke der Verarbeitung**
- Beschreibung der **Kategorien betroffener Personen**
- Beschreibung der **Kategorien personenbezogener Daten** (aus Unterlage 1 Landkarten)
- Beschreibung der **Kategorien von Empfängern**, denen personenbezogene Daten offengelegt werden
- Beschreibung der **Übermittlung** von personenbezogenen Daten **an ein Drittland** oder eine **internationale Organisation**
- Dokumentierung der **geeigneten Garantie dieser Drittländer** oder Organisationen
- Wenn möglich, die **Fristen für die Löschung** der verschiedenen Datenkategorien
- Wenn möglich, die **allgemeine Beschreibung der technischen und organisatorischen Massnahmen** gemäss Art. 32 Ab. 1 DSGVO

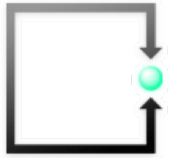


Verzeichnis der Verarbeitungstätigkeiten (2)

Art. 30 (1) DSGVO
Verzeichnis der Verarbeitungstätigkeiten - Verantwortlicher

Jeder Verantwortliche führen ein **Verzeichnis aller Verarbeitung**stätigkeiten. Dieses enthält folgende Angaben:

- **Namen und Kontaktdaten** des **Verantwortlichen**
- **Namen und Kontaktdaten** des **Datenschutzbeauftragten** oder des **EU-Datenschutz-Vertreters des Verantwortlichen**
- **Zwecke der Verarbeitung**
- Beschreibung der **Kategorien betroffener Personen**
- Beschreibung der **Kategorien personenbezogener Daten** (aus Unterlage 1 Landkarten)
- Beschreibung der **Kategorien von Empfängern**, denen personenbezogene Daten offengelegt werden
- Beschreibung der **Übermittlung** von personenbezogenen Daten **an ein Drittland** oder eine **internationale Organisation**
- Dokumentierung der **geeigneten Garantie dieser Drittländer** oder Organisationen
- Wenn möglich, die **Fristen für die Löschung** der verschiedenen Datenkategorien
- Wenn möglich, die **allgemeine Beschreibung der technischen und organisatorischen Massnahmen** gemäss Art. 32 Ab. 1 DSGVO



Verzeichnis der Verarbeitungstätigkeiten (3)

Art. 30 (2) DSGVO
Verzeichnis der Verarbeitungstätigkeiten – Verantwortlicher

- Verzeichnis der Verarbeitungstätigkeiten muss **schriftlich geführt** werden.
- Kann auch in einem **elektronischen Format** erfolgen (3)

- Verzeichnis muss den **Aufsichtsbehörden auf deren Anfrage hin zur Verfügung gestellt** werden (4).

- Verzeichnis muss nicht geführt werden von Unternehmen oder Einrichtungen (5), die weniger als 250 Mitarbeiter beschäftigen, **es sei denn**:

Scheinausnahme

  - Die von ihnen vorgenommene Verarbeitung **birgt ein Risiko** (Achtung: nicht „hohes Risiko“) für die Rechte und Freiheiten der betroffenen Personen
  - Die **Verarbeitung erfolgt nicht nur gelegentlich**
  - Es erfolgt eine Verarbeitung **besonderer Datenkategorien** gemäss Art. 9 Abs. 1 DSGVO
    - Rassische Herkunft, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeiten, genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

Verzeichnis der Verarbeitungstätigkeiten (4)

Beilage 06

Das Verarbeitungsverzeichnis

Verzeichnis von Verarbeitungstätigkeiten
nach Art. 30 EU-Datenschutz-Grundverordnung
(DS-GVO)

www.bitkom.org

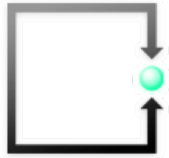
bitkom

Verzeichnis der Verarbeitungstätigkeiten (5)

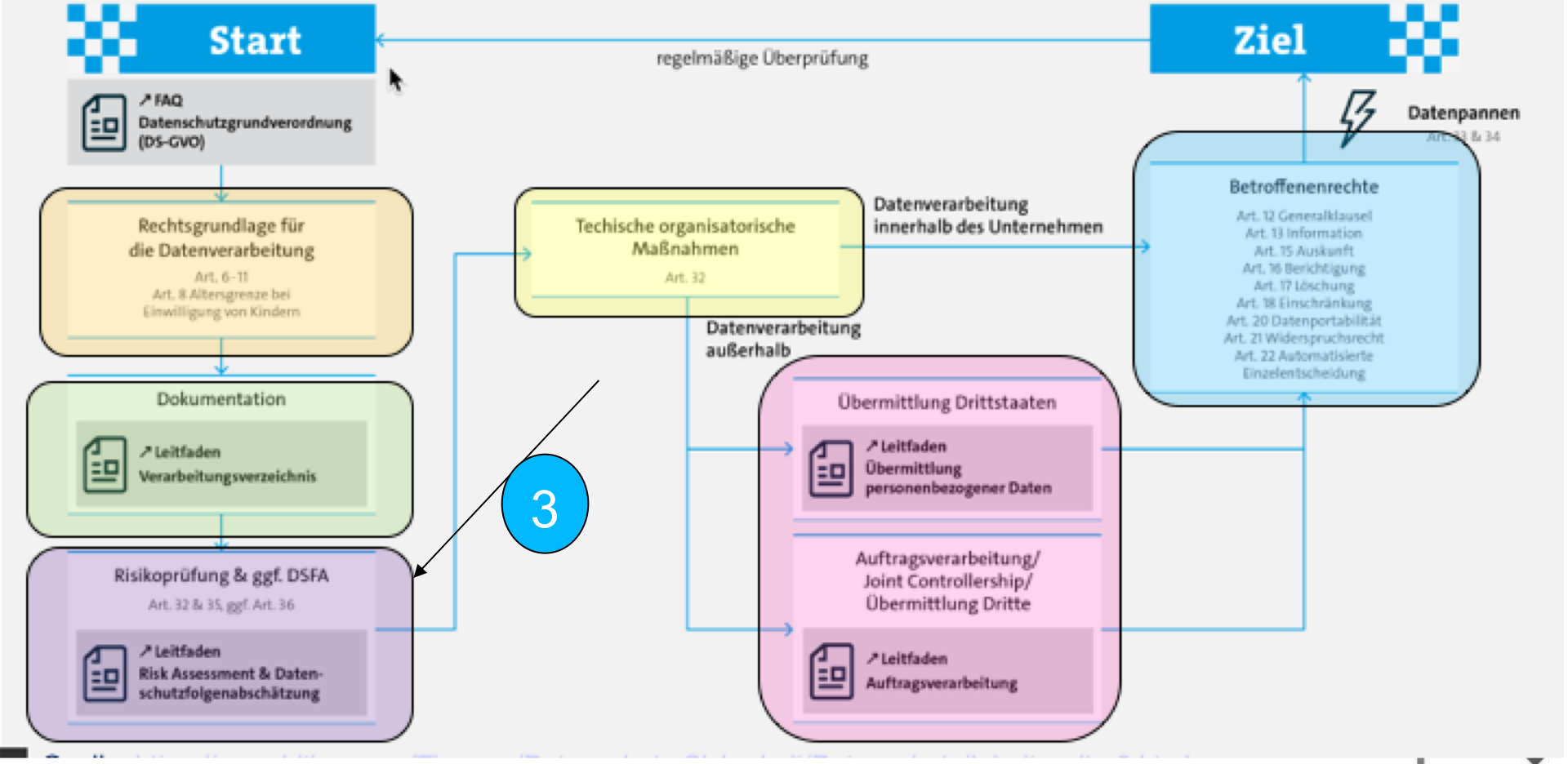
Art. 30 (1) DSGVO
Verzeichnis der Verarbeitungstätigkeiten - Auftragsverarbeiter

Jeder Auftragsverarbeiter führt ein **Verzeichnis aller Verarbeitungstätigkeiten.** Dieses enthält folgende Angaben:

- **Namen und Kontaktdaten** des Auftragsverarbeiters
- Namen und Kontaktdaten jedes Verantwortlichen, für welche der Auftragsverarbeiter personenbezogene Daten verarbeitet,
- Beschreibung der **Kategorien der Verarbeitungen**, die **im Auftrag jedes Verantwortlichen** durchgeführt werden,
- Beschreibung der **Übermittlung von personenbezogenen Daten an ein Drittland** oder eine internationale Organisation
- **Dokumentierung der geeigneten Garantie** dieser Drittländer oder Organisationen
- Wenn möglich, eine **allgemeine Beschreibung** der **technischen und organisatorischen Massnahmen** gemäss Art. 32 Ab. 1 DSGVO



Art. 5 Datenschutzprinzipien & Art. 25 Datenschutz durch Technikgestaltung



Datenschutz-Folgeabschätzung

Art. 35 (1) DSGVO
Datenschutz-Folgeabschätzung

(1) Hat eine **Form der Verarbeitung** …… **voraussichtlich** ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche eine **Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge** für den Schutz personenbezogener Daten durch.

(3) Insbesondere in folgenden Fällen zwingend erforderlich:

- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen mittels automatisierter Verarbeitung einschliesslich Profiling und als Grundlage für Entscheidungen dient, die Rechtswirkungen gegenüber natürlichen Personen entfalten;
- Umfangreiche Verarbeitung der besonderen Datenkategorien gemäss Art. 9 Abs. 1 DSGVO
- Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- Gemäss positiver Liste (5) der Aufsichtsbehörden (Kontaktieren)
- Gemäss negative Ausschluss-Liste (6) der Aufsichtsbehörden (Kontaktieren)

Datenschutz-Folgeabschätzung (2)

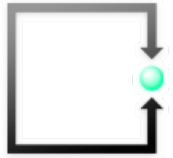
Art. 35 (8) DSGVO
Datenschutz-Folgeabschätzung

(8) Die **Datenschutz-Folgeabschätzung** enthält mindestens Folgendes:

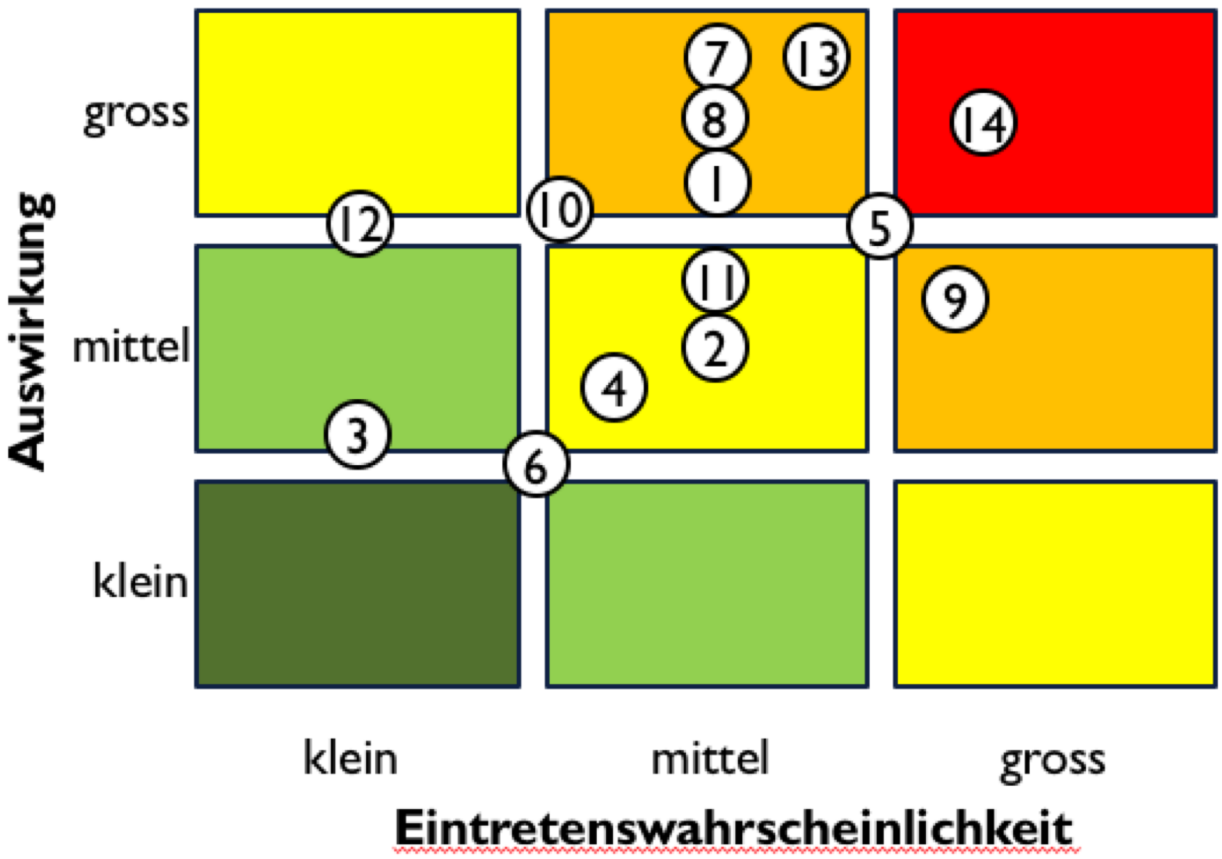
- **Systematische Beschreibung** der geplanten **Verarbeitungsvorgänge**
- **Systematische Beschreibung** der **Zwecke der Verarb**eitung
- **Bewertung der Notwendigkeit** und **Verhältnismässigkeit der Verarbeitungsvorgänge** in Bezug auf den Zweck
- Eine **Bewertung der Risiken** für die Rechte und Freiheiten der betroffenen Personen
- Die zur Bewältigung der Risiken geplanten **Abhilfemassnahmen**

(12) Der **Verantwortliche** führt eine (periodische) **Überprüfung** durch, um zu **bewerten**, ob die **Verarbeitung gemäss der Datenschutz-Folgeabschätzung durchgeführt** wird.

Tipp: einmal jährliche Überprüfung durch GL/VR mit schriftlicher Dokumentation zur Berichterstattung, Beurteilung und angeordneten Massnahmen festhalten.



Datenschutz-Folgeabschätzung (3)

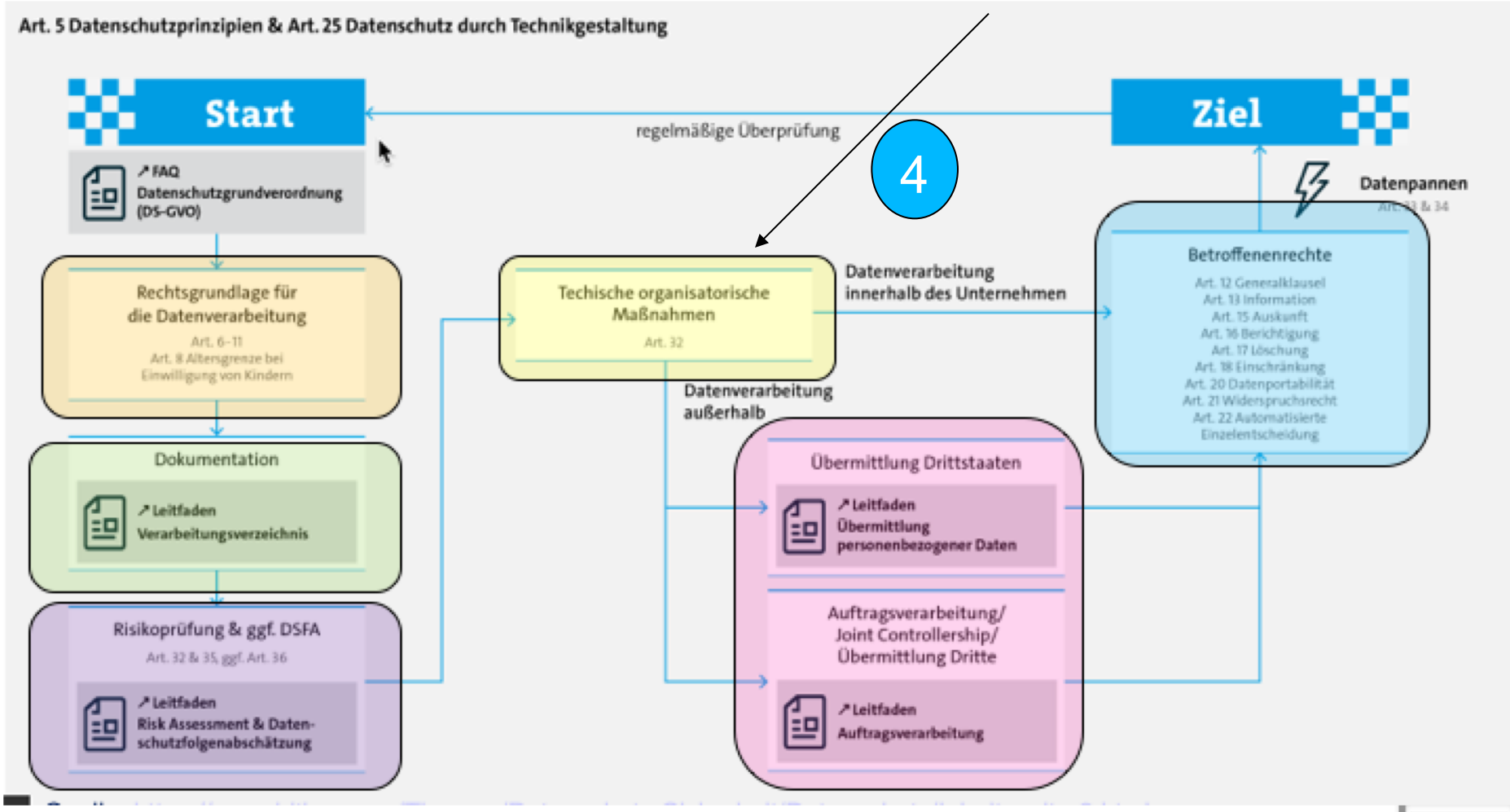


1	Ausfall Know-how Träger
2	Kapazität
3	Personalakquisition
4	Demographie
5	Organisationsform
6	Vorgaben Bund/Kanton
7	Neue Technologien
8	Geschäftsmodell
9	Partner Risiko
10	Kündigung einzelner Kunden
11	.....
12	Investitionsbedarf
13	Projektrisiken
14	Komplexität Infrastruktur

Datenschutz-Folgeabschätzung (4)

Beilage 08
Beilage 10

Organisatorische und technische Massnahmen



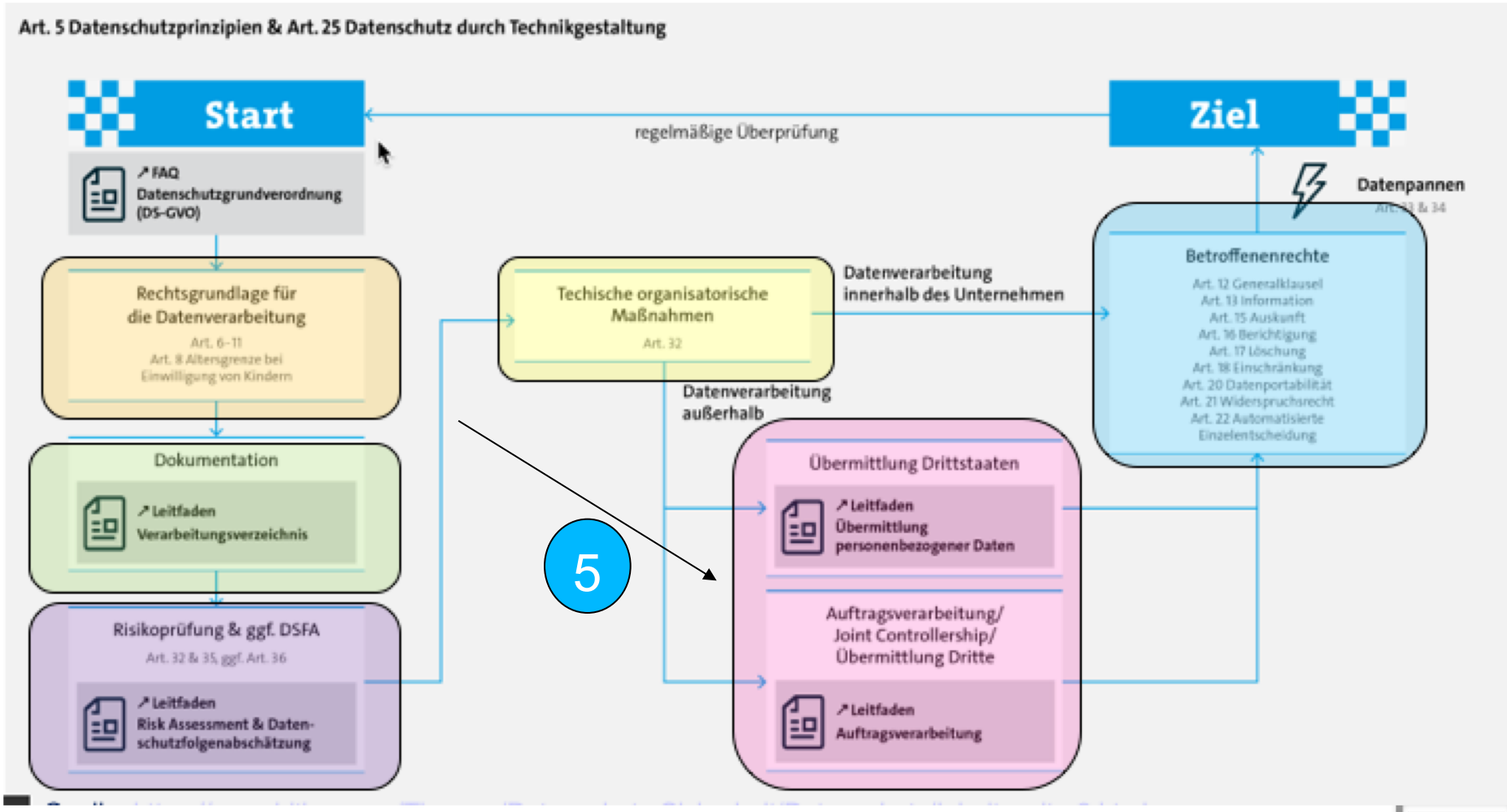
Organisatorische und technische Massnahmen (2)

Art. 32 (1) DSGVO
Sicherheit der Verarbeitung

(1) Der **Verantwortliche** und der **Auftragsverarbeiter** treffen – unter Berücksichtigung des Stands der Technik, der Implementierungskosten, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie des Risikos – **geeignete technische und organisatorische Massnahmen**, um ein **dem Risiko angemessenes Schutzniveau** zu garantieren.

- **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten**,**
- Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer **sicherzustellen,**
- Fähigkeit, die **Verfügbarkeit** personenbezogener Daten und den **Zugang zu ihnen** bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**,
- Unterstellte natürliche Personen **nur auf Anweisung** des Verantwortlichen **Daten verarbeiten**
- Verfahren zur **regelmässigen Überprüfung**, **Bewertung** und **Evaluation der Wirksamkeit** der technischen und organisatorischen Massnahmen

Art. 5 Datenschutzprinzipien & Art. 25 Datenschutz durch Technikgestaltung



Auftragsverarbeiter

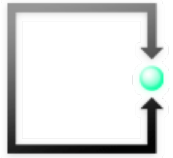
Art. 28 (1) DSGVO
Zusammenarbeit mit Auftragsverarbeiter

Erfolgt eine **Verarbeitung im Auftrag eines Verantwortlichen**, so arbeitet dieser **nur mit Auftragsverarbeitern** zusammen,

- die **hinreichend Garantien** dafür bieten,
- dass **geeignete technische und organisatorische Massnahmen** so durchgeführt werden,
- dass die **Verarbeitung im Einklang mit den Bestimmungen der DSGVO** erfolgt und
- der **Schutz der Rechte der Betroffenen gewährleistet** ist.

Alle Verträge mit Auftragsverarbeitern müssen überprüft und allenfalls angepasst werden

Detailausführungen unter Ziffer 9 vorne



Verarbeitung in Drittländern

Verarbeitung personenbezogener Daten in Drittländern

Version 1.2 | Auf Basis der EU-Datenschutz-Grundverordnung

www.bitkom.org

bitkom

Beilage 09

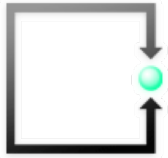
Mehrere Verantwortliche - Regelungspflichten

Festlegung Anwendungsbereich und Verantwortlichkeiten

Die Joint Controllership-Vereinbarung setzt voraus, dass von den gemeinsamen Verantwortlichen zunächst der Anwendungsbereich und die Verantwortlichkeiten festgelegt werden. Folgende Punkte sollten dabei Beachtung finden:

1. Festhalten, dass Vertragsparteien Joint Controllers sind.
2. Aufgabenbeschreibung mit Abgrenzung, welcher Verantwortliche welche Aufgabe übernimmt. Aufteilung der Aufgaben zwischen den Beteiligten sehr operativ beschreiben.
3. Festlegung des Zwecks und der Mittel der Datenverarbeitung

   Beispiel: Betrieb einer gemeinsamen Online-Buchungs-Plattform zwecks Durchführung von Reservierungen und Nutzung der Daten zu gemeinsamen Marketingaktionen.
4. Pflichten des Joint Controller A
5. Pflichten des Joint Controller B



Mehrere Verantwortliche – Regelungspflichten (2)

Checkliste für Verträge zu Joint Controllership

(x) Die Kreuze stellen dar, welcher Verantwortliche, welche Aufgabe übernimmt.

Pflichten aus der DS-GVO	Controller A	Controller A
Festlegung des Zwecks und der Mittel der Datenverarbeitung	x	x
Festlegung der Art der personenbezogenen Daten	x	x
Art. 26 Abs. 1 Festlegung in einer Vereinbarung in transparenter Form, wer welche Verpflichtung gemäß dieser Verordnung erfüllt. Die Vereinbarung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.		
Art. 26 Abs. 1 optional: Angabe einer Anlaufstelle für die betroffenen Personen.		
Art. 26 Abs. 2 Das Wesentliche der Vereinbarung wird dem Betroffenen zur Verfügung gestellt.		
Art. 27 Schriftliche Benennung eines Vertreters in der EU, falls ein Verantwortlicher nicht in der Union niedergelassen ist.		
Art. 13 Informationspflicht bei Erhebung personenbezogener Daten.		
Art. 14 Informationspflicht, wenn Daten nicht bei der betroffenen Person erhoben wurden.		
Art. 15 Bearbeitung von Auskunftsverlangen.		

Mehrere Verantwortliche – Regelungspflichten (3)

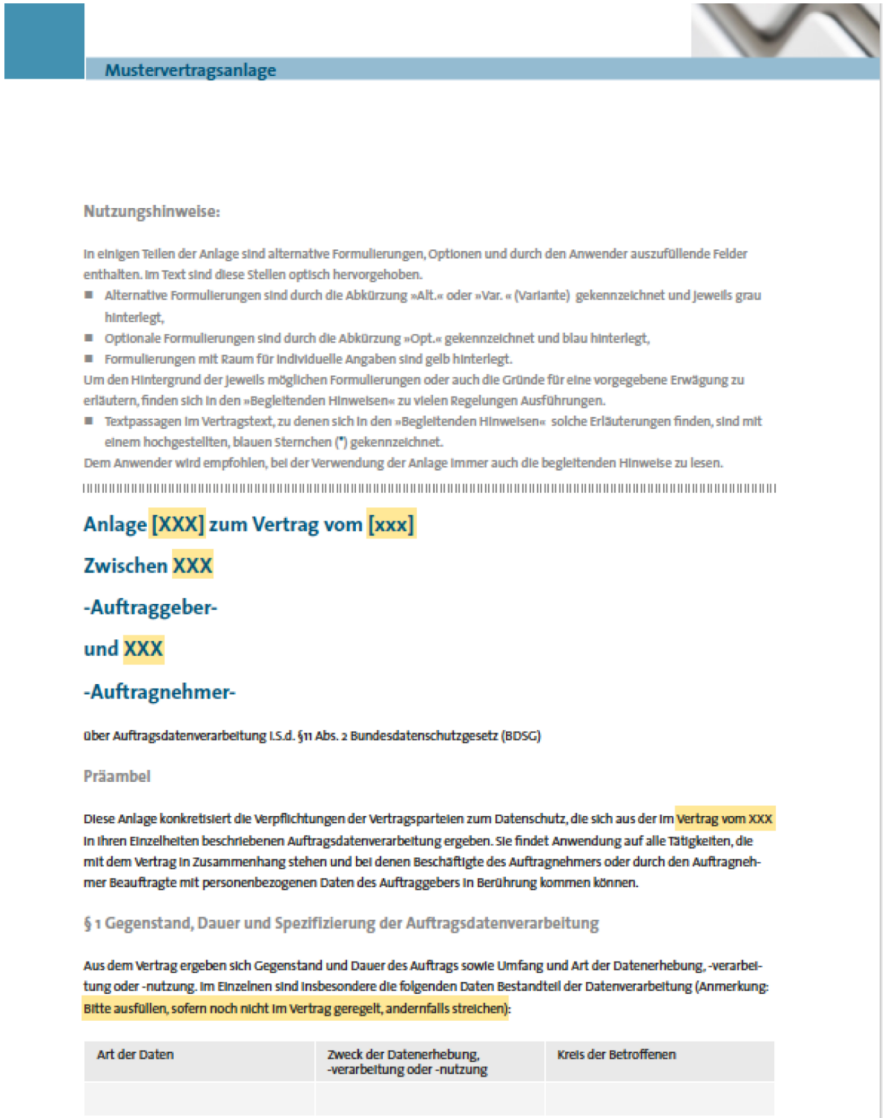
Beilage 11

Musterverträge für Auftragsverarbeiter

Beilage 13

BITKOM

Musterverträge für Auftragsverarbeiter (2)



Mustervertragsanlage

Nutzungshinweise:

In einigen Teilen der Anlage sind alternative Formulierungen, Optionen und durch den Anwender auszufüllende Felder enthalten. Im Text sind diese Stellen optisch hervorgehoben.

- Alternative Formulierungen sind durch die Abkürzung »Alt.« oder »Var. « (Variante) gekennzeichnet und jeweils grau hinterlegt,
- Optionale Formulierungen sind durch die Abkürzung »Opt.« gekennzeichnet und blau hinterlegt,
- Formulierungen mit Raum für individuelle Angaben sind gelb hinterlegt.

Um den Hintergrund der jeweils möglichen Formulierungen oder auch die Gründe für eine vorgegebene Erwägung zu erläutern, finden sich in den »Begleitenden Hinweisen« zu vielen Regelungen Ausführungen.

- Textpassagen im Vertragstext, zu denen sich in den »Begleitenden Hinweisen« solche Erläuterungen finden, sind mit einem hochgestellten, blauen Sternchen (*) gekennzeichnet.

Dem Anwender wird empfohlen, bei der Verwendung der Anlage immer auch die begleitenden Hinweise zu lesen.

Anlage [XXX] zum Vertrag vom [xxx]

Zwischen XXX

-Auftraggeber-

und XXX

-Auftragnehmer-

über Auftragsdatenverarbeitung i.S.d. §11 Abs. 2 Bundesdatenschutzgesetz (BDSG)

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Vertrag vom XXX in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung

Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung (Anmerkung: Bitte ausfüllen, sofern noch nicht im Vertrag geregelt, andernfalls streichen):

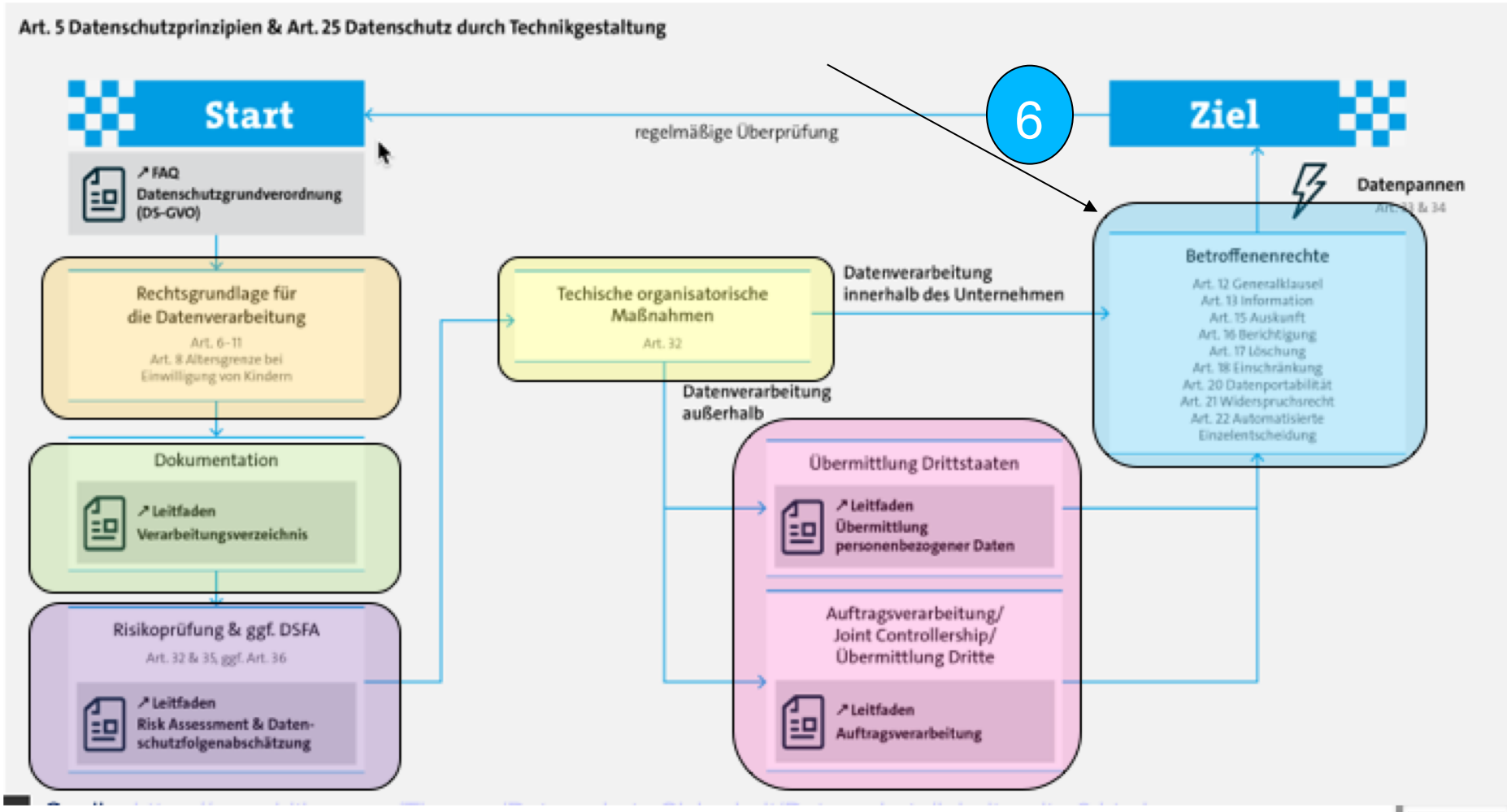
Art der Daten	Zweck der Datenerhebung, -verarbeitung oder -nutzung	Kreis der Betroffenen

Empfehlung

Verträge mit Auftragsverarbeiter müssen von erfahrenen Juristen ausgearbeitet und geprüft werden.

Das Haftungsrisiko bei unkontrollierter Übernahme von kopierten Vertragsmustern ist viel zu hoch.

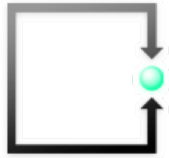
Prozesse bezüglich Betroffenenrechte



Prozesse bezüglich Betroffenenrechte (2)

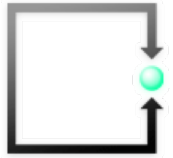
Im 6. Schritt geht es darum, dass das **Unternehmen** in Bezug auf die **Abwicklung der Prozesse** für alle **vorhandenen Betroffenenrechte** vorbereitet ist.

- Prozesslandkarte
- Dokumentierte Prozessbeschreibung (Nachweisdokumente)
- Prozesseigner festgelegt und ausgebildet
- Kontinuierliche Überprüfung und Verbesserung der Prozesse



Prozesse bezüglich Betroffenenrechte (3)

Was heisst „Daten löschen“ genau?



Prozesse bezüglich Betroffenenrechte (4)

Art. 17 DSGVO – Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Der **Betroffene** hat das **Recht** vom **Verantwortlichen zu verla**ngen, dass er betreffende **personenbezogene Daten unverzüglich löscht** und der Verantwortliche ist verpflichtet, diese Daten **unverzüglich** zu löschen, sofern einer der **folgenden Gründe** zutrifft:

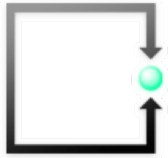
(1a) Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig;
(1b) Die betroffene Person hat ihre ausdrückliche Einwilligung widerrufen
(1c) Die betroffene Person legt Widerspruch gegen eine weitere Verarbeitung ein und es liegen keine vorrangigen Gründe für eine Weiterverarbeitung vor
(1d) Daten wurden unrechtmässig verarbeitet
(1e) Daten müssen gemäss EU-Recht oder Länderrecht gelöscht werden

Prozesse bezüglich Betroffenenrechte (5)

Art. 17 DSGVO – Recht auf Löschung („Recht auf Vergessenwerden“)

(3) Der **Verantwortliche** kann sich gegen eine Löschung wehren, wenn die weitere Verarbeitung erforderlich ist,

- Zur Ausübung des Rechts auf freie Meinungsäusserung und Information;
- **Zur Erfüllung einer rechtlichen Verpflichtung** (z.B. gesetzliche Aufbewahrungspflichten?)
- Zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt (z.B. Strafregister) erfolgt,
- Aus Gründen des öffentlichen Interesses im Bereich öffentliche Gesundheit
- Für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche, historische oder statistische Zwecke
- **Zur Geltendmachung, Ausübung oder Verteidigung von Rechts-ansprüchen**



Leitfaden
zum Sicheren Datenlöschen

Version 2.0

Beilage 14

BITKOM

FSDZ RECHTSANWÄLTE & NOTARIAT AG

An alle interessierten DatenschützerInnen

DSGVO: PERSONENBEZOGENE DATEN LÖSCHEN ART. 17 DSGVO WIE DENN?

Baar, 8.2.2018
Von: Lukas Fässler, Rechtsanwalt & Informatikexperte

/Users/lukasfassler/Desktop/DSGVO Art. 17 Daten löschen/DSGVO - Daten Löschen - 08-02-2018.docx

Aufgrund der EU-Datenschutz-Verordnung (DSGVO) müssen Unternehmen immer wissen, wo Daten zu Personen gespeichert sind (Register der personenbezogenen Daten), um diese bei Bedarf auf Antrag der natürlichen Person zu löschen.
Dies dürfte vorerst noch eine ziemlich schwer zu meisternde Herausforderung sein.

1. Gesetzliche Grundlage

Zuerst sollte man den Gesetzestext kennen. Deshalb hier Art. 17 DSGVO nachfolgend:

1. Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:
a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Assoziierte selbständige Rechtsanwältin:

Eva Patroncini
lic.iur. Rechtsanwältin[1,3]
Fachanwältin SAV für Arbeitsrecht
Industriestrasse 7
CH-8610 Uster
Tel.: +41 44 380 85 85
patroncini@fsdz.ch

Partnerkanzleien:

Lichtsteiner Rechtsanwälte und Notare
Urs Lichtsteiner
lic. iur. Rechtsanwalt[1,3], MSc (Stanford)
lichtsteiner@lilaw.ch
Nadja Eggerschwiler
M.Law Rechtsanwältin und Notarin[1,3]
eggerschwiler@lilaw.ch

Baarerstrasse 10, Postfach 7517
CH-6302 Zug
Tel.: +41 41 726 90 00
Fax: +41 41 726 90 05
www.lilaw.ch
info@lilaw.ch
UID: CHE-404.805.335 MWST

Anwaltskanzlei Dr. Weltert
Hans M. Weltert
Dr. iur. Rechtsanwalt[1,4]
hans.weltert@rsweltert.ch
Matthias Heim
lic.iur. Rechtsanwalt[1,4]
matthias.heim@rsweltert.ch
Michael Heim
lic.iur. Rechtsanwalt[1,4]
michael.heim@rsweltert.ch

Bahnhofstrasse 10
CH-5001 Aarau
Tel.: +41 62 832 77 33
Fax: +41 62 832 77 34
www.rsweltert.ch
info@rsweltert.ch
UID: CHE-100.877.506 MWST

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug
[3] Eingetragen im Anwaltsregister des Kantons Zürich
[4] Eingetragen im Anwaltsregister des Kantons Aargau

Beilage 15

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Beilage 16

Empfehlung zur Vernichtung von Personendaten

Herausgeber:

Datenschutzstelle
Städtle 38
Postfach 684
9490 Vaduz

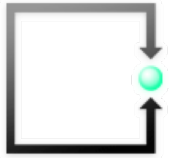
Fürstentum Liechtenstein

T +423 236 60 90

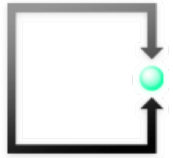
info.dss@llv.li
www.dss.llv.li

Version 1.0 / September 2017

11
Spezialfragen



11.1
Sind Daten im Fürstentum Liechtenstein auch der DSGVO unterstellt?



DSGVO und Fürstentum Liechtenstein

FSDZ RECHTSANWÄLTE & NOTARIAT AG

An alle interessierten DatenschützerInnen

DSGVO:
ANWENDBARKEIT IN LIECHTENSTEIN

Baar, 8.2.2018
Von: Lukas Fässler, Rechtsanwalt & Informatikexperte

/Users/lukasfassler/Desktop/Anwendbarkeit Liechtenstein/DSGVO - Anwendbarkeit Liechtenstein - 08-02-2018.docx

Schweizerische Unternehmen unterstehen der DSGVO, wenn sie Waren oder Dienstleistungen an Kunden in der EU anbieten (Art. 3 Abs. 2 lit. a DSGVO).

Wie verhält es sich, wenn ich in einem Online-Shop Waren oder Dienstleistungen an **Kunden in Liechtenstein** anbiete?

Es gibt noch keine abschliessende Antwort dazu. Zwischenstand der Rechtslage ist aber folgende:

- Liechtenstein ist nicht Mitgliedstaat der EU. Somit wird die DSGVO nicht unmittelbar anwendbar.
- Liechtenstein ist Mitglied des EWR (gemeinsam mit Island und Norwegen). Gegenwärtig läuft der Übernahmeprozess der DSGVO durch den EWR[1].
- Sollte die Übernahme der DSGVO in das EWR-Abkommen beschlossen werden, wäre der nächste Verfahrensschritt der Entwurf eines Übernahmebeschlusses durch den ‚Gemischten Ausschuss'. Nach Inkrafttreten des Übernahmebeschlusses würde dieser in das EWR-Abkommen aufgenommen werden und die DSGVO würde in Liechtenstein unmittelbare Anwendung finden (keine nationale Umsetzung).
- Damit wäre dann auch ihr Art. 3 Abs. 2 lit. a anwendbar, so dass die Ansprache liechtensteinischer Kunden im Ergebnis zur Anwendung der DSGVO auf den entsprechenden Anbieter führen würde.
- Solange dies noch nicht geschehen ist, gilt das Datenschutzgesetz des Fürstentums Liechtenstein[2]

[1] http://www.efta.int/eea-lex/l/%5b0%5d=field_annex_chapter%3A776&f%5b1%5d=field_annex_chapter%3A941
[2] https://www.gesetze.li/konso/2002.55

Lukas Fässler
lic.iur.Rechtsanwalt[1,2], Informatikexperte
faessler@fsdz.ch

Zugerstrasse 76b
CH-6340 Baar
Tel.: +41 41 727 60 80
Fax: +41 41 727 60 85
www.fsdz.ch
sekretariat@fsdz.ch
UID: CHE-349.787.199 MWST

Assoziierte selbständige Rechtsanwältin:
Eva Patroncini
lic.iur. Rechtsanwältin[1,3]
Fachanwältin SAV für Arbeitsrecht
Industriestrasse 7
CH-8610 Uster
Tel.: +41 44 380 85 85
patroncini@fsdz.ch

Partnerkanzleien:
Lichtsteiner Rechtsanwälte und Notare
Urs Lichtsteiner
lic. iur. Rechtsanwalt[1,3], MSc (Stanford)
lichtsteiner@lilaw.ch
Nadja Eggerschwiler
MLaw Rechtsanwältin und Notarin[1,3]
eggerschwiler@lilaw.ch
Bleicherstrasse 10, Postfach 7517
CH-6302 Zug
Tel.: +41 41 726 90 00
Fax: +41 41 726 90 05
www.lilaw.ch
info@lilaw.ch
UID: CHE-404.805.335 MWST

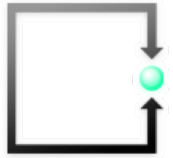
Anwaltskanzlei Dr. Weltert
Hans M. Weltert
Dr. iur. Rechtsanwalt[1,4]
hans.weltert@raweltert.ch
Matthias Heim
lic.iur. Rechtsanwalt[1,4]
matthias.heim@raweltert.ch
Michael Heim
lic.iur. Rechtsanwalt[1,4]
michael.heim@raweltert.ch
Bahnhofstrasse 10
CH-5001 Aarau
Tel.: +41 62 832 77 33
Fax: +41 62 832 77 34
www.raweltert.ch
info@raweltert.ch
UID: CHE-100.877.506 MWST

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug
[3] Eingetragen im Anwaltsregister des Kantons Zürich
[4] Eingetragen im Anwaltsregister des Kantons Aargau

Beilage 17

https://www.fsdz.ch/file-docs/dsgvo_-_anwendbarkeit_liechtenstein_-_08-02-2018.pdf

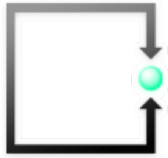
11.2
Was ist mit Cookies-Einsatz (Profiling-Daten)?



Ausdrückliche Einwilligung für mehrere Kanäle

Der BGH hat im **Urteil vom 1.2.2018, III ZR 196/17** neu Folgendes festgehalten**:**

- Es braucht in jedem Fall eine ausdrückliche Einwilligung
- Das Markieren eines Feldes in einem Online-Shop kann dieses Kriterium erfüllen (Clickwrapping - "Klickkasten-Einwilligung")
- Die Einwilligung muss für den Konsumenten klar sein, d.h. er muss wissen für welche Produkte und Dienstleistungen welcher Unternehmung er einwilligt
- Wirksame Einwilligung darf keine anderen Erklärungen oder Hinweise enthalten als die konkrete Zustimmungserklärung
- Es braucht also eine ausdrückliche und gesonderte Erklärung
- Die Widerspruchhinweis darf nicht fehlen
- In dieser Erklärung kann der Konsument somit auch für mehrere Kanäle in einer Erklärung zustimmen.



Ausdrückliche Einwilligung für mehrere Kanäle (2)

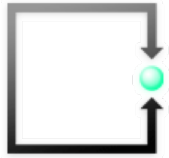
Muster für ausdrückliche Mehrkanal-Einwilligung

„ich möchte künftig über neue Angebote und Services der X. AG per E-Mail, Telefon, Fax, SMS, MMS…….. Persönlich informiert und beraten werden.

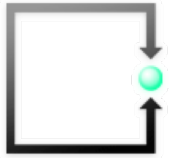
Ich bin damit einverstanden, dass meine Vertragsdaten aus meinen Vertragen mit der X. AG von dieser bis zum Ende des jeweiligen Vertragsjahres, das auf die Beendigung des entsprechenden Vertrages folgt, zur individuellen Kundenberatung (und Bewerbung) verwendet werden.

Meine Vertragsdaten sind die bei der X AG zur Vertragserfüllung (Vertragsabschluss, -änderung, -beendigung, Abrechnung von Entgelten) erforderlichen und freiwillig abgegebenen Daten.

Ich nehme zur Kenntnis, dass ich diese ausdrückliche Einwilligung jederzeit und ohne Begründungen gegenüber der X. AG mündlich, schriftlich (Brief) oder elektronisch (E-Mail, SMS, MMS, WhatsApp etc.) widerrufen kann. Ab diesem Zeitpunkt ist die X. AG nicht mehr berechtigt, meine Daten für die Information oder Beratung über neue Angebote oder Services zu benutzen.



11.3
ePrivacy-Verordnung EU



EUROPÄISCHE
KOMMISSION

Ab 25. Mai 2018 EU-weit in Kraft

Brüssel, den 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Beilage 20

Vorschlag für eine

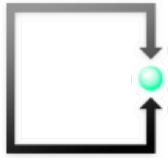
VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)

Schwerpunkte neues EU- Datenschutzrecht (2)

ePrivacy-Verordnung

- Januar 2017 Vorschlag EU-Kommission für eine VO zu Schutz von Daten in der elektronischen Kommunikation.
- Ergänzt DSGVO
- Adressaten: natürliche und juristische Personen, soweit diese **Dienstleistungen der elektronischen Kommunikation** anbieten oder nutzen (WhatsApp, Facebook, Skype usw).
- **Schutz** umfasst den **kommunizierten Inhalt** sowie die **Metadaten** (Anrufzeitpunkt, Standortdaten usw.).
- Geltungsbereich: Adressaten der elektronischen Kommunikationsdienstleistungen bzw. Endbenutzer befinden sich in der EU
- Vertraulichkeit als Standard für die elektronische Kommunikation in der EU
- Third Party Tracking durch Cookies ist verboten. Ausnahme ausdrückliche Einwilligung des Endnutzers liegt vor und ist nachweisbar.



Schwerpunkte neues EU- Datenschutzrecht (2)

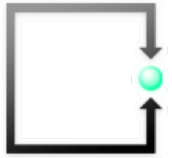
ePrivacy-Verordnung

- **Unerbetene elektronische Kommunikation** unabhängig der Form (E-Mails, SMS, Newsletter, Telefonanrufe usw.) ist **verboten**, sofern nicht **ausdrückliche Zustimmung** des Konsumenten vorliegt (Opt-In). Einwilligung muss **nachweisbar** sein.

- Einwilligung muss jederzeit widerrufbar sein. Separater Hinweis in jeder elektronischen Kommunikation (AGB, DSB, Subscribe in Newslettern etc.)

- Werbeanrufe müssen die Rufnummer anzeigen oder eine Vorwahl (0900) anzeigen, die auf Werbung hinweist.

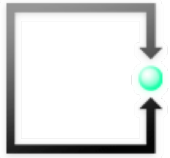
- Wird am 25. Mai 2018 (mit DSVGO) gleichzeitig in Kraft treten.



Weitere Sonderbestimmungen der EU

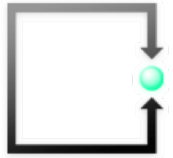
11.4

Gibt es noch andere Sonderbestimmungen der EU, die zu berücksichtigen sind?

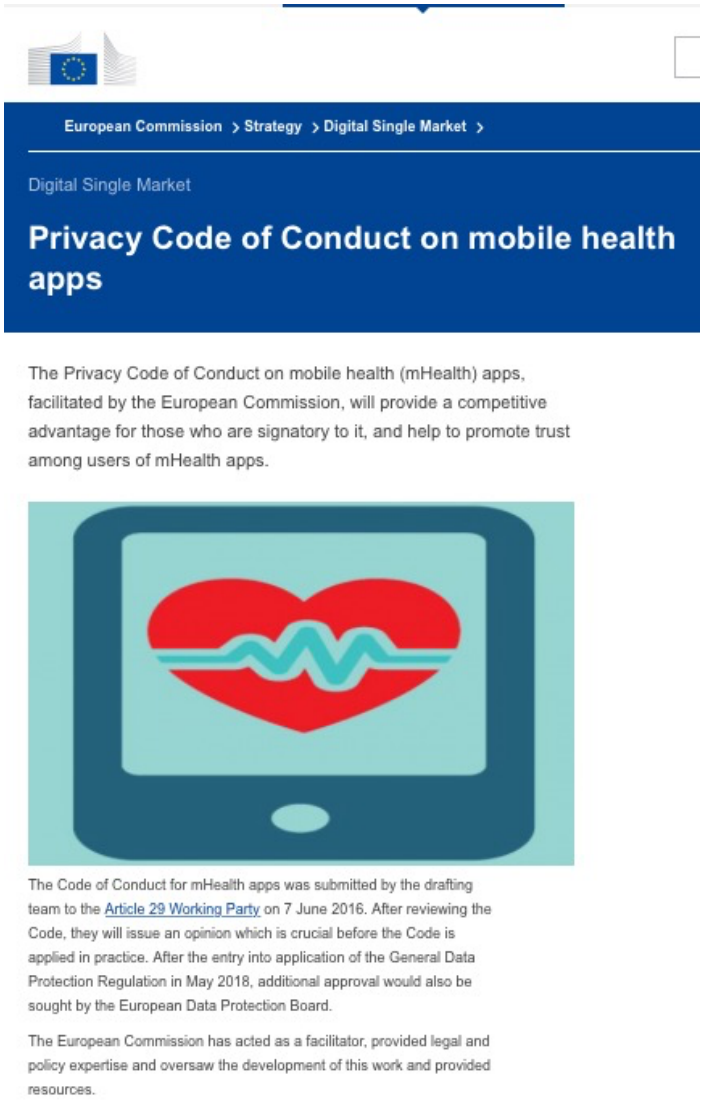


Weitere Sonderbestimmungen der EU

Privacy Code of Conduct on mobile health apps



Weitere Sonderbestimmungen der EU (2)



European Commission > Strategy > Digital Single Market >

Digital Single Market

Privacy Code of Conduct on mobile health apps

The Privacy Code of Conduct on mobile health (mHealth) apps, facilitated by the European Commission, will provide a competitive advantage for those who are signatory to it, and help to promote trust among users of mHealth apps.

The Code of Conduct for mHealth apps was submitted by the drafting team to the Article 29 Working Party on 7 June 2016. After reviewing the Code, they will issue an opinion which is crucial before the Code is applied in practice. After the entry into application of the General Data Protection Regulation in May 2018, additional approval would also be sought by the European Data Protection Board.

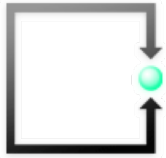
The European Commission has acted as a facilitator, provided legal and policy expertise and oversaw the development of this work and provided resources.

- http://bit.ly/215zwiv

Schwerpunkte neues EU- Datenschutzrecht (3)

EU-Code of Conduct on mobile health applications

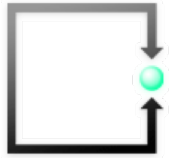
- Softlaw: Befolgung freiwillig, aber State of the art
- Adressaten: natürliche und juristische Personen, die mHealth-Anwendungen herstellen.
- Ziel: datenschutzrechtliche Mindestanforderungen bei der Bearbeitung von Personendaten mittels mHealth-Apps.
- App kann man auf Konformität überprüfen lassen -> Aufnahme in zentrales EU-Register
- INHALT: Einwilligung der Nutzer, Datensparsamkeit, Privacy by Design and Default, Datenzugangs- und Berichtigungsrecht der Nutzer, Aufbewahrungsdauer von Daten, technische und organisatorische Massnahmen für IT-Sicherheit, Transfer von Daten ins Ausland, Vorgehen bei Datenschutzverletzungen
- Soll am 25. Mai 2018 (mit DSVGO) gleichzeitig in Kraft treten.



EU-Datenschutz-Vertreter

11.5

Wie und wann muss ich einen EU-Datenvertreter bezeichnen?

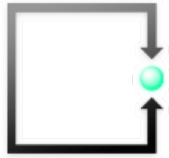


EU-Datenschutz-Vertreter (2)

Nach Art. 27 DSGVO benötigen Schweizer Unternehmen, welche personenbezogene Daten von natürlichen Personen mit Niederlassung in der EU verarbeiten oder verarbeiten lassen (Auftragsverarbeiter) zwingend einen **Datenschutz-Vertreter** in der EU.

Insbesondere **CH-Online-Shops**, welche Waren oder Dienstleistungen an Konsumenten in EU-Länder verkaufen.

Der Vertreter muss in dem Land niedergelassen sein, in dem der Käufer wohnt oder in das die Waren exportiert werden.



EU-Datenschutz-Vertreter (3)

https://e-comtrust.ch/file-docs/auftrag_fuer_eu-datenschutz-vertreter_-_version_2-00_-_05-03-2018.pdf

e-comtrust international

Datenschutz-Vertreter in der Europäischen Union (EU)

CH-Onlineshopbetreiber brauchen ihn

e-comtrust international ag
Zugerstrasse 76B
CH-6340 Baar
Tel: ++41 +41 727 00 70
Fax: ++41 +41 727 60 85
www.e-comtrust.ch
sekretariat@e-comtrust.ch

Viele Schweizer Unternehmen müssen die neue Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) am 25. Mai 2018 umsetzen und benötigen deshalb unter anderem auch einen Datenschutz-Vertreter in der EU. Dies betrifft insbesondere Schweizerische Online-Shopbetreiber, welche Ihre Waren oder Dienstleistungen[1] an Konsumenten, die sich in der EU befinden, anbieten oder deren Verhalten (mit Cookies oder anderen Marketing-Tools) beobachten.[2]

Pflicht für CH-Onlineshop-Betrei
Gemäss Art 27 DSGVO muss in d
in der Union benennen. Der Vertr
Im Zusammenhang mit den Ihnen

Der Vertreter wird durch den Ver
betroffene Personen bei sämtlich
Wenn Sie nicht selber eine Niede
Sie einen solchen Datenschutz-V

Hinweis: Ausnahmsweise wird kein D
schützenswerten Daten betrifft, und
Freiheiten natürlicher Personen führt.
freizeichnen.

[1] Angebote umfassen sämtliche Dienstleis
ausdrücklich betroffen. Es genügt auch b

[2] Die DSGVO findet gemäss Art. 3 DSGVO
Verantwortliches oder Auftragsverarb
a) betroffenen Personen in der
Zahlung zu leisten ist;
b) das Verhalten betroffener P

Beilage 18

e-comtrust international

e-comtrust international ag
Zugerstrasse 76B
CH-6340 Baar
Tel: ++41 +41 727 00 70
www.e-comtrust.ch
fuerzielflieger.ch

Beilage 19

Auftrag für die Bestellung eines EU-Datenschutz-Vertreters nach Art. 27 DSGVO

Die Unterzeichnenden bestellen gestützt auf Art. 27 DSGVO einen **EU-Datenschutz-Vertreter** nach Art. 27 DSGVO gemäss den nachfolgenden Angaben.

Es gelten folgende Bestimmungen gemäss Art. 27 DSGVO:

3. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die betroffenen Personen, deren personenbezogene Daten im Zusammenhang mit den ihnen angebotenen Waren oder Dienstleistungen verarbeitet werden oder deren Verhalten beobachtet wird, sich befinden.

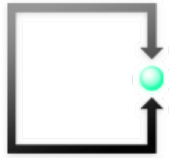
4. Der Vertreter wird durch den Verantwortlichen oder den Auftragsverarbeiter beauftragt, zusätzlich zu diesem oder an seiner Stelle insbesondere für Aufsichtsbehörden und betroffene Personen bei sämtlichen Fragen im Zusammenhang mit der Verarbeitung zur Gewährleistung der Einhaltung dieser Verordnung als Anlaufstelle zu dienen.

5. Die Benennung eines Vertreters durch den Verantwortlichen oder den Auftragsverarbeiter erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Verantwortlichen oder den Auftragsverarbeiter selbst.

Der Auftrag wird unter folgenden allgemeinen Geschäftsbedingungen ausgeführt:

Dokument	/Users/lukasfaessler/Desktop/EU Datenschutz-Vertreter/Auftrag für EU-Datenschutz-Vertreter - Version 2-00 -05-03-2018.docx
Version:	1.10
Datum:	05.03.2018
Ersetzt Dokument vom:	Version 1.00 vom 5.2.2018
Autor:	Lukas Fässler, e-comtrust International ag, Artherstrasse 20, 6300 Zug
Letzte Änderung von:	05-03-2018

11.6
Wo gibt es weiterführende Unterlagen und Informationen?



www.e-comtrust.ch

www.eu-datenschutz-vertreter.ch

www.fsdz.ch

Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch

Profil Kompetenzen Team Aktuell Publikationen Referenzen Kontakt

Aktuelles aus unserer Kanzlei.

Alle Intern Publikationen Veranstaltungen

Seminar DSGVO Datenschutz-Grundverordnung

Verfasst am 01.03.2018
Ab dem 25. Mai 2018 ist die neue Datenschutz-Grundverordnung DSGVO direkt anwendbar und muss bis dann von den Unternehmungen umgesetzt werden.

Was muss wirklich umgesetzt werden? Was muss veranlasst werden? Und wer ist wofür verantwortlich?

Antworten zu diesen Fragen gibt das Praxisseminar DSGVO an der Fachhochschule Nordwestschweiz FHNW in Basel.
››Weiterlesen

Änderungen bei Nachnahmegebühren ab März 2018

Verfasst am 28.02.2018
Viele Menschen bezahlen ihre Einkäufe beim Online-Shopping per Nachnahme. Hier gibt es ab März 2018 eine Änderung. Bisher waren bei der Bezahlung per Nachnahme bei der DHL zwei Gebühren fällig: ein Nachnahmeentgelt zusätzlich zum Paketpreis sowie ein Übermittlungsentgelt.

Hier gibt es ab März 2018 eine neue Regelung.

››Weiterlesen

Jetzt anrufen 041 727 60 80
oder E-Mail schreiben

FSDZ Rechtsanwälte & Notariat AG

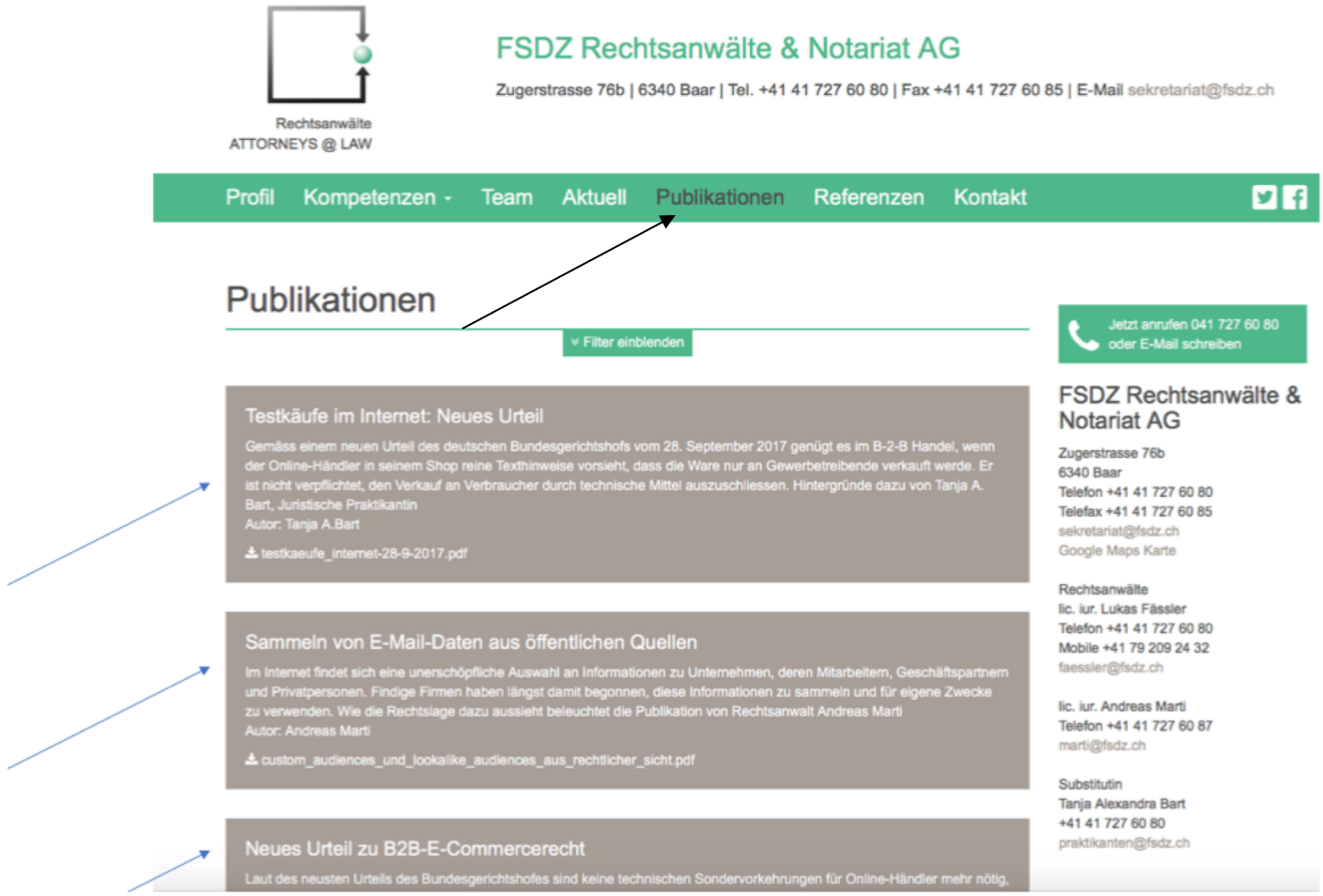
Zugerstrasse 76b
6340 Baar
Telefon +41 41 727 60 80
Fax +41 41 727 60 85
sekretariat@fsdz.ch
Karte Google Maps

Rechtsanwalt
lic. iur. Lukas Fässler
Telefon +41 41 727 60 80
Mobile +41 79 209 24 32
faessler@fsdz.ch

Substitut
Philipp A. Keller
Telefon +41 41 727 60 80
praktikanten@fsdz.ch

Assoziierte selbständige
Anwälte:

www.fsdz.ch


Rechtsanwälte
ATTORNEYS @ LAW
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 | E-Mail sekretariat@fsdz.ch
Profil
Kompetenzen
Team
Aktuell
Publikationen
Referenzen
Kontakt
Publikationen
Filter einblenden
Testkäufe im Internet: Neues Urteil
Gemäss einem neuen Urteil des deutschen Bundesgerichtshofs vom 28. September 2017 genügt es im B-2-B Handel, wenn der Online-Händler in seinem Shop reine Texthinweise vorsieht, dass die Ware nur an Gewerbetreibende verkauft werde. Er ist nicht verpflichtet, den Verkauf an Verbraucher durch technische Mittel auszuschliessen. Hintergründe dazu von Tanja A. Bart, Juristische Praktikantin
Autor: Tanja A.Bart
testkaeufe_internet-28-9-2017.pdf
Sammeln von E-Mail-Daten aus öffentlichen Quellen
Im Internet findet sich eine unerschöpfliche Auswahl an Informationen zu Unternehmen, deren Mitarbeitern, Geschäftspartnern und Privatpersonen. Findige Firmen haben längst damit begonnen, diese Informationen zu sammeln und für eigene Zwecke zu verwenden. Wie die Rechtslage dazu aussieht beleuchtet die Publikation von Rechtsanwalt Andreas Marti
Autor: Andreas Marti
custom_audiences_und_lookalike_audiences_aus_rechtlicher_sicht.pdf
Neues Urteil zu B2B-E-Commercerecht
Laut des neusten Urteils des Bundesgerichtshofes sind keine technischen Sondervorkehrungen für Online-Händler mehr nötig,
Jetzt anrufen 041 727 60 80
oder E-Mail schreiben
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76b
6340 Baar
Telefon +41 41 727 60 80
Telefax +41 41 727 60 85
sekretariat@fsdz.ch
Google Maps Karte
Rechtsanwälte
lic. iur. Lukas Fässler
Telefon +41 41 727 60 80
Mobile +41 79 209 24 32
faessler@fsdz.ch
lic. iur. Andreas Marti
Telefon +41 41 727 60 87
marti@fsdz.ch
Substitutin
Tanja Alexandra Bart
+41 41 727 60 80
praktikanten@fsdz.ch

Besten Dank

Lukas Fässler
Rechtsanwalt & Informatikexperte
FSDZ Rechtsanwälte & Notariat AG
Zugerstrasse 76B
6340 Baar / Zug
+41 41 727 60 80
www.fsdz.ch
faessler@fsdz.ch

@LukasFaessler