



🏠 ▶ + ▶ Wirtschaft ▶ CAS Digitalisierung und Digitale Führun...

CAS Digitalisierung und Digitale Führung im HRM

Weiterbildung

Wirtschaft

Alle CAS Wirtschaft ▶

Alle Weiterbildungen Personalmanagement und Organisation ▶

◀ Alle Weiterbildungen

Digitale Verantwortung: Datenschutz und Compliance



Wochentag	Datum	Zeit	Thema	Dozent
Cluster 1 – Digitale Unternehmenswelt und digitale Unternehmensführung				
Tag 1	DO 08.09.2022	09.00 – 10.00	Einführung in Kurs und Vorstellung	Frederik Thomas & Gery Bruederlin, FHNW
		10.00 – 12.15	Grundlagen der digitalen Transformation	Frederik Thomas, FHNW
		13.00 – 17.00	Leitlinien der digitalen Unternehmensführung	Frederik Thomas, FHNW
Tag 2	DO 22.09.2022	09.00 – 17.00	Agile Leadership – Haltung und Kultur Grundlagen der Agilen Führung und Projektmanagement	Martin König, FHNW
Tag 3	DO 06.10.2022	09.00 – 12.15	Digitale Leadership; Kompetenzen und Methoden	Frederik Thomas, FHNW
		13.00 – 17.00	Digitale Verantwortung: Datenschutz & Compliance	Lukas Fässler, FSDZ
Tag 4	DO 20.10.2022	09.00 – 17.00	Methodologien im digitalen Kontext	Frederik Thomas, FHNW



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

[Impressum](#) [Datenschutzbestimmungen](#)

[Profil](#) [Kompetenzen](#) [Team](#) [Aktuell](#) [Publikationen](#) [Referenzen](#) [Kontakt](#)



Umsetzung der DSGVO

[Hinweis schliessen](#)

Als Anwaltskanzlei mit Schwerpunkt vor allem im Datenschutzrecht ist uns ein verantwortungsbewusster Umgang mit Ihren personenbezogenen Daten wichtig. FSDZ Rechtsanwälte & Notariat AG verzichtet vollständig auf den Einsatz von Social Media-Plugins, Websiteanalyse-Diensten und Anzeigen sowie Marketing-Diensten (keine Cookies, keine Google Analytics etc.). Sie können ohne Angabe von personenbezogenen Daten unsere Webseite besuchen.

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

Rechtsanwältin und Notarin
lic. iur. Carmen de la Cruz Böhringer
Telefon +41 41 727 60 80
sekretariat@fsdz.ch

Assoziierte selbständige Anwältin:

Eva Patroncini
Büro Uster
Imkerstasse 7
Postfach 1280
CH-8610 Uster
Telefon +41 44 380 85 85
patroncini@fsdz.ch

Partnerkanzlei de la
cruz beranek Rechtsanwälte
AG, Zug
de la cruz beranek Rechtsanwälte AG
Industriestrasse 7
CH 6300 Zug
Telefon: +41 41 710 28 50

www.fsdz.ch





Lukas Fässler Rechtsanwalt

Rechtsanwalt und Informatikexperte,
Certified Software Asset Manager IAITAM Inc.

Profil

1975 – 1980	Studium an der Universität Fribourg/CH	VRP AR Informatik AG	(2019)
1982	Anwaltspatent des Kantons Luzern	Vizepräsident VR ILZ OW/NW	(2001)
1982 – 1984	Gerichtsschreiber am Amtsgericht Hochdorf	Vizepräsident VR HIN AG	(2000)
1984 - 1987	Gerichtsschreiber am Verwaltungsgericht Luzern	Präsident Verein SSGI	(2005)
1987 - 1992	EDV-Beauftragter im Gerichtswesen Kanton Luzern	VRP Viacar AG	(2010-2012)
1992 - 1997	Informatikchef des Kantons Luzern	Dozent Fachhochschule NW in Basel	
1997	Selbständiger Spezialanwalt seit September 1997	Dozent Universität Basel	
1999 - 2000	Universität Zürich, Nachdiplomstudium, Internationales Wirtschaftsrecht (Spezialisierungskurs Immaterialgüterrecht, Technologie- und Informationsrecht)	Dozent Universität Bern/Lausanne	
2017	"Certified Software Asset Manager IAITAM Inc." bei der International Association of Information Technology Asset Managers Inc. in Amerika		

Continuity, der Verantwortung und Haftung sofort auf den Tisch



Cloud-Rechenzentrum der OVN in Strassburg am 10.3.2021

Cyberangriff auf Comparis

Comparis-Hacker hatten Zugang zu Nutzerdaten

Donnerstag, 12.07.2019, 05:24 Uhr
Aktualisiert um 08:28 Uhr

<https://www.srf.ch/news/wirtschaft/cyberangriff-auf-comparis-comparis-hacker-hatten-zugang-zu-nutzerdaten>

Cyberkriminalität

Emil Frey-Gruppe wurde Opfer von Cyberangriff

Mittwoch, 12.01.2022, 01:44 Uhr

<https://www.srf.ch/news/schweiz/cyberkriminalitaet-emil-frey-gruppe-wurde-opfer-von-cyberangriff>

Hacker legen einzige Zeitungspapierfabrik der Schweiz lahm – Folgen nicht absehbar

<https://www.watson.ch/digital/schweiz/744582672-hacker-legen-einzig-zeitungspapierfabrik-der-schweiz-lahm-mit-folgen>

Hackerangriff auf die Rothenburger Auto AG Group

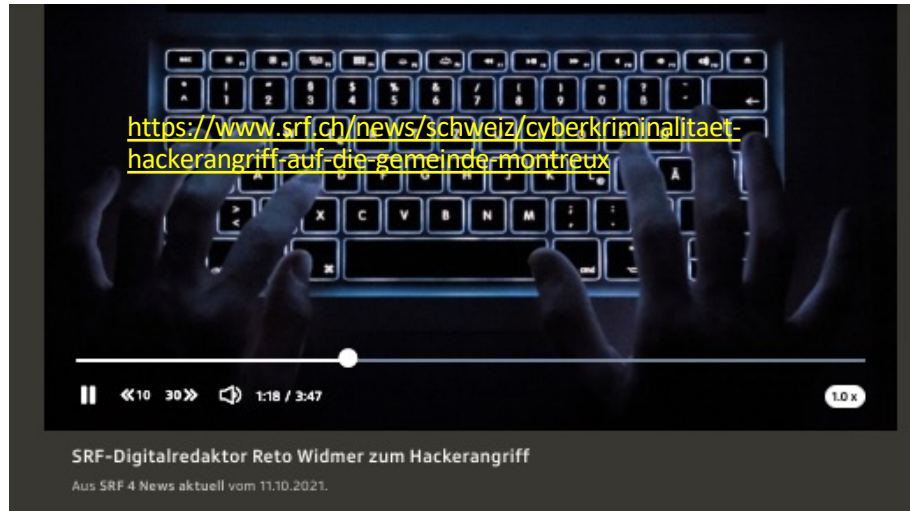
Die Auto AG Group mit Sitz in Rothenburg wurde Opfer eines Hackerangriffs. Die Täterschaft ist bisher unbekannt.

27.08.2019, 17.26 Uhr

Merken Drucken Teilen



Das Gebäude der Auto AG Group in Rothenburg. (Bild: Nadia Schärli, Rothenburg, 16. April 2019)



News > Schweiz >

Quelle:

<https://www.srf.ch/news/schweiz/cyberkriminalitaet-hackerangriff-auf-die-gemeinde-montreux>

Cyberkriminalität

Hackerangriff auf die Gemeinde Montreux

Montag, 11.10.2021, 08:17 Uhr
Aktualisiert um 11:33 Uhr



Dieser Artikel wurde 4-mal geteilt.

- Die Waadtländer Gemeinde Montreux ist Ziel eines Cyberangriffs geworden.
- Die Attacke sei am Sonntagmorgen entdeckt worden, teilte die Gemeinde mit. Die Grösse des Angriffs und der Schaden können erst jetzt eingeschätzt werden, teilt die Gemeinde mit.

SPAM-MAILS

Hackerangriff auf Apotheker

APOTHEKE ADHOC, 11.01.2014 09:37 Uhr



Gefälschte E-Mail: Ein Hacker will mit Daten aus dem Postfach eines Apothekers Kasse machen.

Foto: APOTHEKE ADHOC

Berlin - Nach einem Hackerangriff wurde einem Apotheker aus Niedersachsen nicht nur das Passwort geknackt – ein bislang Unbekannter hat auch im Namen von Dr. Rainer Camehn in einer E-Mail um Geld gebeten. Noch ist der Hackerangriff auf das Postfach des

Teil 1

Digitale Verantwortung im Unternehmen und in öffentlichen Verwaltungen



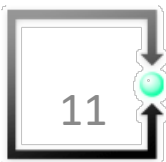
Die digitale Verantwortung

- Applikationen und digital unterstützte Prozesse im Unternehmen sind nicht mehr wegzudenken.
- Es besteht eine vollständige Abhängigkeit von der Digitalisierung im Unternehmen.
- Damit stellt die Digitalisierung vollständig neue Anforderungen an die strategischen (Verwaltungsrat) und operativen Führungskräfte (Geschäftsleitung) einer Unternehmung.
- Die Digitalisierung ist ein zentraler Wirtschaftlichkeitsfaktor, aber zugleich ein erheblicher Risikofaktor im Unternehmen, die mit aller Sorgfalt zu steuern, überwachen, verbessern und nach den geltenden Bestimmungen (Compliance; z.B. neues Datenschutzrecht ab 2022) auszurichten ist.

Nachfolgende Ausführungen zur Aktiengesellschaft gelten sinngemäss auch für die Träger öffentlicher Aufgaben (Verwaltungen).

Hier sind jedoch die jeweiligen Organisations-, Verantwortlichkeits- und Haftungsgesetze des Bundes, der Kantone oder – soweit relevant – der Gemeinden zu beachten.

Öffentliche-rechtliche Aktiengesellschaften, Anstalten oder andere juristische Personen des öffentlichen Rechts unterstehen in der Regel einer Spezialgesetzgebung (z.B. AR: eGov-Gesetz; ILZ OW/NW: Konkordatsvereinbarung der Kantone OW und NW), wobei jeweils die privatrechtlichen Verantwortlichkeitsbestimmungen zur Anwendung gebracht werden.



Die gesetzlichen Grundlagen zur Unternehmensführung

Die digitalen Sorgfaltspflichten der Führungskräfte

VR - Verwaltungsrat Strategische Führung

Art. 716a⁴³⁰

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 Geschäftsberichtes⁴³¹ 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.

VR - Verwaltungsrat
Strategische Führung

B. Der Verwaltungsrat⁴¹⁴

5. die Obergaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;

Compliance-Verantwortung

VR - Verwaltungsrat
Strategische Führung

B. Der Verwaltungsrat⁴¹⁴

Art. 717⁴³³

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.

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

vom 30. März 1911 (Stand am 1. Juli 2015)

III. Haftung für
Verwaltung,
Geschäfts-
führung und
Liquidation

Art. 754⁴⁸⁸

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.



Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Urteilkopf

139 III 24

4. Auszug aus dem Urteil der I. zivilrechtlichen Abteilung i.S. A. und Mitb. gegen X. AG
(Beschwerde in Zivilsachen)
4A_375/2012 vom 20. November 2012

Regeste a

Art. 754 OR; aktienrechtliche Verantwortlichkeit.

Haftung des Verwaltungsrats für die Kosten eines erfolglos geführten Prozesses über die Eintragung von Namenaktien im Aktienbuch der Gesellschaft, in dem erkannt wurde, die Verweigerung der Eintragung sei nicht im Interesse der Gesellschaft erfolgt und habe gegen das Gleichbehandlungsgebot der Aktionäre sowie gegen das Rechtsmissbrauchsverbot verstossen (E. 3).



Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

3.2 Nach Art. 717 Abs. 1 OR müssen die Mitglieder des Verwaltungsrats, sowie Dritte, die mit der Geschäftsführung befasst sind, ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der

Gesellschaft in guten Treuen wahren. Die gesetzlich normierte Treuepflicht verlangt, dass die Mitglieder des Verwaltungsrats ihr Verhalten am Gesellschaftsinteresse ausrichten. Für die Sorgfalt, die der Verwaltungsrat bei der Führung der Geschäfte der Gesellschaft aufzuwenden hat, gilt ein objektiver Massstab. Die Verwaltungsräte sind zu aller Sorgfalt verpflichtet und nicht nur zur Vorsicht, die sie in eigenen Geschäften anzuwenden pflegen (**BGE 122 III 195 E. 3a S. 198; BGE 113 II 52 E. 3a S. 56**). Das Verhalten eines Verwaltungsratsmitglieds wird deshalb mit demjenigen verglichen, das billigerweise von einer abstrakt vorgestellten, ordnungsgemäss handelnden Person in einer vergleichbaren Situation erwartet werden kann (PETER BÖCKLI, Schweizer Aktienrecht, 4. Aufl. 2009, § 13 N. 575).

Die Sorgfalt richtet sich nach dem Recht, Wissensstand und den Massstäben im Zeitpunkt der fraglichen Handlung oder Unterlassung. Bei der Beurteilung von Sorgfaltspflichtverletzungen hat mithin eine ex ante Betrachtung stattzufinden (vgl. Urteile 4A_74/2012 vom 18. Juni 2012 E. 5.1; 4A_467/2010 vom 5. Januar 2011 E. 3.3; BERNARD CORBÖZ, in: Commentaire romand, Code des obligations, Bd. II, 2008, N. 22 zu **Art. 754 OR**; GERICKE/WALLER, in: Basler Kommentar, Obligationenrecht, Bd. II, 4. Aufl. 2012, N. 31c zu **Art. 754 OR**; WATTER/PELLANDA, in: Basler Kommentar, Obligationenrecht, Bd. II, 4. Aufl. 2012, N. 6 zu **Art. 717 OR**).

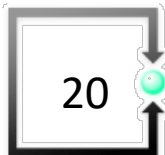
Grobfahrlässigkeit

Grobfahrlässig handelt, wer grundlegende Vorsichtsgebote nicht beachtet, die eine vernünftige Person in der gleichen Situation befolgt hätte und dadurch andere Personen und auch sich selbst in Gefahr bringt. Zur Grobfahrlässigkeit im Strassenverkehr zählen demnach alle Situationen, bei denen man eine grobe Verletzung der Verkehrsregeln begeht, wie also das Überfahren einer Sicherheitslinie oder das Missachten eines Stoppsignals.

Was sind die Folgen von grobfahrlässigem Handeln?

Grobfahrlässigkeit wirkt sich auf die Versicherungsleistung bei einem Schadenfall aus. Eine Versicherung hat so das Recht, einen Teil der entstandenen Kosten von der grobfahrlässig handelnden Person zurückzuerlangen. Das wird auch als Regress oder Rückgriffsrecht bezeichnet. Je nach Schwere der Grobfahrlässigkeit kann dieser Anteil zum Beispiel 20%, 50% oder auch mehr betragen.

Eine Organhaftpflichtversicherung gibt somit keine umfassende Schadensdeckung. Regress bei Grobfahrlässigkeit in den AVB regelmässig vorgesehen.



Gesetzliche Beweislastumkehr zulasten
Führungskräfte (VR und GL)

Wer seine laufend aktualisierten
Sorgfaltmassnahmen (Auswahl, Unterrichtung und
Überwachung nicht) nicht beweisen kann, haftet.



Meineimpfung.ch

Das BAG ist nicht verantwortlich – **ist das wirklich so?**



- Datensicherheit: Rein Sache der privaten Stiftung
- Nie über Sicherheitslücken informiert worden
- Im Stiftungsrat sitzt die Leiterin der Sektion Infektionskontrolle (in privater Funktion)
- Eidg. Finanzkontrolle ist Revisionsstelle

<https://www.srf.ch/play/radio/echo-der-zeit/audio/datenschutzprobleme-bei-der-plattform-meineimpfungen-ch?id=fbbd88e3-0b77-4a1e-8c53-38cd4a92b443>

Standards und Normen

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

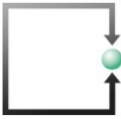
vom 30. März 1911 (Stand am 1. Januar 2016)

Art. 962 OR

4 Das oberste Leitungs- oder Verwaltungsorgan ist für die Wahl des anerkannten Standards zuständig, sofern die Statuten, der Gesellschaftsvertrag oder die Stiftungsurkunde keine anderslautenden Vorgaben enthalten oder das oberste Organ den anerkannten Standard nicht festlegt.



swiss code of best practice for corporate governance



Swiss Code of Best Practice

Seit dem 1. Juli 2002 existiert zudem der **Swiss Code of Best Practice** (oder "*Swiss Code*") vom Dachverband der Schweizer Wirtschaft (**economiesuisse**). Dieser listet Verhaltensregeln auf, die für eine vorbildliche Corporate Governance notwendig sind. Die Anwendung des Codes basiert auf Freiwilligkeit. Dieser Swiss Code of Best Practice wurde 2007 um zehn Empfehlungen zur Vergütung von Verwaltungsräten und oberstem Management erweitert.^[8]

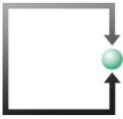


Aufgaben des Verwaltungsrats

9

Der von den Aktionären gewählte Verwaltungsrat nimmt die Oberleitung und Oberaufsicht der Gesellschaft bzw. des Konzerns wahr.

- Der Verwaltungsrat bestimmt die strategischen Ziele, die generellen Mittel zu ihrer Erreichung und die mit der Führung der Geschäfte zu beauftragenden Personen.
- Der Verwaltungsrat prägt die Corporate Governance und setzt diese um.
- Er sorgt in der Planung für die grundsätzliche Übereinstimmung von Strategie, Risiken und Finanzen.
- Der Verwaltungsrat lässt sich vom Ziel der nachhaltigen Unternehmensentwicklung leiten.



Umgang mit Risiken und Compliance, internes Kontrollsystem

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

20

- 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.



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

21

- 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.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE
Digital Innovation Office

Bericht vom 28 Juni 2021

Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung

Datum: 28 Juni 2021

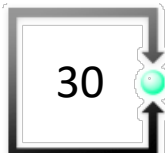
Ort: Bern

Auftraggeberin:

Bundesamt für Energie BFE
CH-3003 Bern
www.bfe.admin.ch

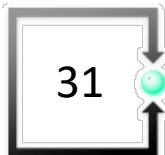
Auftragnehmer/in:

Deloitte AG
General-Guisan-Quai 38, CH-8022 Zürich
www.deloitte.com/ch



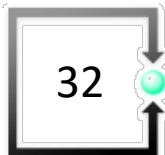
Feststellungen mit Adressierung der Sorgfaltspflichten

- Zunehmende Anwendung digitaler Technologien (dig. Monitoring- und Steuerungssysteme, Einsatz intelligenter Messsysteme (Smart Meter) oder Internet-of-things-Technologien (IoT).
- Verschmelzung der Informationstechnologie (IT) mit der operationellen Technologie-Landschaft (OT).
- Trennung beider Welten IT und OT ist nicht mehr gegeben und es entstehen daher **neue, bisher nicht da gewesene Angriffsvektoren**.
- Entsprechend **steigt die potentielle Cyber-Bedrohungslage** und die damit **verbundenen Risiken rasant**
- **Existierende Schutzkonzepte müssen der neuen Ausgangslage und den technologischen Entwicklungen angepasst werden.**



Fazit

- Die gesamte Digitalisierung mit allen Facetten im Unternehmen ist einer **periodischen Risikobeurteilung** in vielfacher Hinsicht zu unterziehen:
 - Sicherstellung der Business Continuity (Verfügbarkeit)
 - Absicherung der Infrastrukturen, Daten (Infrastructure and data security)
 - Einhaltung von Branchenvorgaben (z.B. Elektrizitätswirtschaft als kritischer Faktor für die Landesversorgung -> Standards und Vorgaben der Bundesbehörden oder der Branche.
 - Einbindung in das IKS (interne Kontrollsystem der Unternehmung)
 - Periodizität nachweisen (mindestens jährlich einmal)



Teil 2

Grundlagen des neuen Datenschutz- und Datensicherheitsrechts

(DSGVO und nDSG-CH)

Grundprinzipien des neuen europäischen Datenschutzes (DSGVO)

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.

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.

- **Ist am 25.5.2018 in Kraft getreten**

- 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 / alle anderen Länder: nur Schutz der Personendaten natürlicher Personen)



VERORDNUNGEN

Datenschutz-Grundverordnung ab 2018

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)

Verordnungstext mit Erwägungen

4.5.2016

DE

Amtsblatt der Europäischen Union

L 119/1

<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:

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 (*) 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.

(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).

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

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.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

BBI 2020
www.bundesrecht.admin.ch
Massgebend ist die signierte
elektronische Fassung



Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]

vom 25. September 2020

Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

vom ...

Der Schweizerische Bundesrat,

gestützt auf die Artikel 8 Absatz 3, 10 Absatz 4, 12 Absatz 5, 16 Absatz 3, 25 Absatz 6, 28 Absatz 3, 33, 59 Absätze 2 und 3 des Bundesgesetzes vom 25. September 2020¹ über den Datenschutz (DSG)

verordnet:



Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Streichung: Schutz der Daten
juristischer Personen

Art. 2 Persönlicher und sachlicher Geltungsbereich

¹ Dieses Gesetz gilt für die Bearbeitung von Personendaten **natürlicher Personen** durch:

a. private Personen;

Unternehmen sind auch private Personen

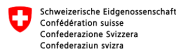
b. Bundesorgane.

Kantone erlassen 26 Kantons-DSG

² Es ist nicht anwendbar auf:

- Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;
- Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

Umsetzung in der CH



[Signature]

[QR Code]

Anhang
**Bundesgesetz
über den Datenschutz**
(Datenschutzgesetz, DSG)

Vorentwurf

vom ...

- Vernehmlassung zum Gesetzesentwurf lief bis 4. April 2017
 - Botschaft des Bundesrates an das Parlament am 15.9.2017
 - Behandlung im Nationalrat und Ständerat: Beginn 12.6.2018 NR
- **Parlament hat nDSG am 25.9.2020 verabschiedet**
- **Bundesrat hat die Verordnung zum neuen Datenschutzgesetz am 23.6.2021 in Vernehmlassung geschickt. Wurde in der Zwischenzeit überarbeitet und publiziert.**
- Der Bundesrat hat Datenschutzgesetz, Verordnung zum Datenschutzgesetz und eine Zertifizierungs-Verordnung am 31.8.2022 **in Kraft gesetzt auf den 1.9.2023**
 - <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-90134.html>

Geltungsbereich Bund – Kantone - Private

Schlussabstimmung im Bundesparlament in Bern für das
Eidg. Datenschutzgesetz

25. September 2020

CH-DSG gilt für

- Bundesbehörden und
- Private (natürliche Personen und Unternehmen)

Kantone erlassen jetzt laufend ihre 26 (!!) neuen kantonalen DSG für ihre kantonalen Verwaltungen, ihre eigenen öffentlich-rechtlichen Körperschaften (z.B. Spitäler, Gebäudeversicherung, Informatikbetriebe, EW etc.) und die Gemeinden.

Bundesverfassung der Schweizerischen Eidgenossenschaft

101

vom 18. April 1999 (Stand am 3. März 2013)

Art. 13 Schutz der Privatsphäre

¹ Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

² Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

vom 10. Dezember 1907 (Stand am I. Juli 2013)

Art. 28³⁰

II. Gegen
Verletzungen
1. Grundsatz

¹ Wer in seiner Persönlichkeit widerrechtlich verletzt wird, kann zu seinem Schutz gegen jeden, der an der Verletzung mitwirkt, das Gericht anrufen.

² Eine Verletzung ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

**Warum kann die DSGVO (EU) für
ihr Unternehmen relevant sein?**

Markortprinzip

Angebot an Bürger in EU - Aufenthalt in EU - BEOBACHTEN

Art. 3 DSGVO

Räumlicher Anwendungsbereich

- (2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
- a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
 - b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

Anknüpfungspunkt 1

Angebot von Waren und Dienstleistungen (Art. 3 Abs. 2 lit.a DSGVO)

Anknüpfungspunkt 2

Überwachung des Verhaltens von Personen in der EU (Art. 3 Abs. 2 lit.b DSGVO)

Analyse-Tools - Tracking-Tools – Social media plugins

Immer, wenn durch **Analyse-Tools** (z.B. temporäre oder permanente Cookies), **Tracking** (Beobachten, Sammeln, Auswerten des Surfverhaltens von Patienten) oder **Profiling** (Erstellen von Profilen von Patienten, um bestimmte persönliche Merkmale wie Leistung, Gesundheit, Aufenthaltsort etc. zu bewerten oder vorherzusagen), **Social Plugins** oder **Schaltflächen** wie „Like-Button“ von Facebook oder „Follower“ von Twitter und Instagram oder „Merken“ von Pinterest, die individuelle Rückverfolgbarkeit der Patienten ermöglicht wird oder zum Zweck der individuellen Werbung erfolgt, dann liegt BEOBACHTEN vor. Dazu gibt es auch bereits weitreichende höchstrichterliche Rechtsprechung z.B. des Deutschen Bundesgerichtshofes oder des Europäischen Gerichtshofes EuGH⁷.

Tracking – Cookies etc.

Die meisten Internetseiten setzen heute standardmässig Analysetools jeder Ausprägung ein (z.B. Google-Analytics, Google Fonts etc.).

Das ist BEOBACHTEN von BETROFFENEN

- **Analysetools abschalten**
- **Neue Datenschutzbestimmungen (DSB) verfassen,**
 - **Transparenz- und Koppelungsverbot sicherstellen,**
 - **Widerruf einbinden und**
 - **AUSDRÜCKLICHES EINVERSTÄNDNIS via clickwrapping (z.T. schon auf der Eintrittsseite) abholen und speichern.**

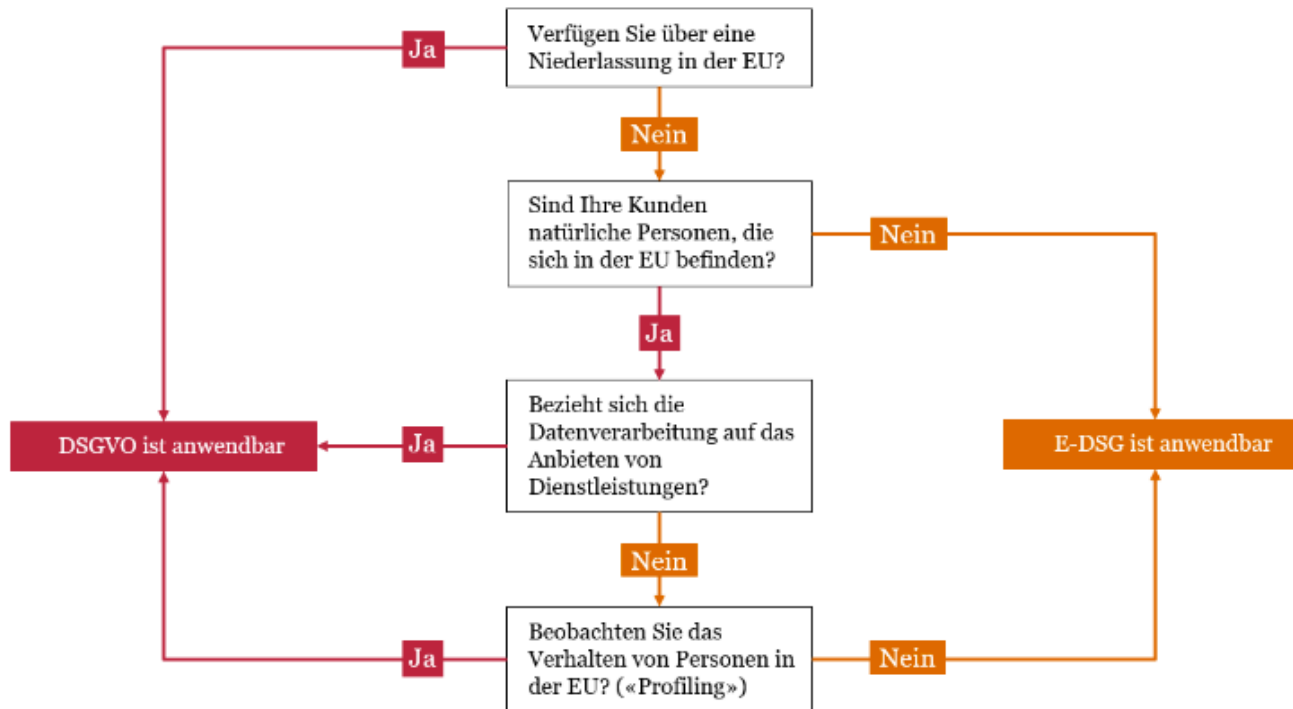
Webseiten-Scanning zu Cookies-Einsatz

Ist-Zustand

Land	Unternehmen	Produkt und Verbindungs-URL
US	Cloudflare, Inc.	CDNJS https://cdnjs.cloudflare.com/ajax/libs/fancybox/3.5.7/jquery.fancybox.min.css
US	Cloudflare, Inc.	Cloudflare CDN https://unpkg.com/aos@2.3.1/dist/aos.css
US	Google Ireland Limited	Google Analytics https://region1.google-analytics.com/gcollect?v=2&tid=G-5B9CD73C8R&gtm=2oe9q0&_p=1504670904&cid=1855430335.1664458288&ul=en-us&sr=800x600&uaa=&uab=&uafvl=&uamb=0&uam=&uap=&uapv=&uaw=0&_z=ccd.v9B&_s=2&sid=1664458287&sct=1&seg=1&dl=https%3A%2F%2Fwww.fairway-asset.com%2Fweekly-thoughts%2Ffly-me-to-the-moon&dt=Fly%20Me%20to%20the%20Moon%20%20Weekly%20Thoughts%20-%20Fairway%20Asset%20Management&en=user_engagement&_et=23019
US	Google Ireland Limited	Google CDN https://www.gstatic.com/recaptcha/releases/ovmhLiigaw4D9ujHYHcKkP/recaptcha_en.js
US	Google Ireland Limited	Google Fonts https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2
US	Google Ireland Limited	Google Tag Manager https://www.googletagmanager.com/gtag/js?id=G-5B9CD73C8R&l=dataLayer&cx=c
US	Google Ireland Limited	Google reCAPTCHA https://www.google.com/recaptcha/api.js?render=6Lchoz4aAAAAAGMSgmz8yhjQRuCXnOKJ6l-k1Ilt
US	jQuery	jQuery CDN https://code.jquery.com/ui/1.12.1/jquery-ui.min.js



Entscheidungsbaum Geltungsbereich



Quelle: https://www.pwc.ch/de/publications/2018/Datenschutz_in_der_Schweiz.pdf

DSGVO-Pflichten für Unternehmen und Sanktionen

Spezialvorschrift DSGVO: Datenschutz-Vertreter 27 DSGVO

Datenschutz-Vertreter nach Art. 27 DSGVO

(1) In den Fällen gemäß Artikel 3 Absatz 2 benennt der Verantwortliche oder der Auftragsverarbeiter **schriftlich einen Vertreter in der Union.**

(2) Diese Pflicht gilt nicht für

- a) eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder
- b) Behörden oder öffentliche Stellen.

(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.

Pflicht zur Bestellung eines EU-Datenschutz-Vertreters für CH-Unternehmen



When trust is on your side

HOME DIENSTLEISTUNGEN URTEILE INFO BLOG ÜBER UNS KONTAKT IMPRESSUM DATENSCHUTZBESTIMMUNGEN

EU-Datenschutzvertreter nach Art. 27 DSGVO

e-comtrust international ag stellt Ihrem Unternehmen einen Datenschutz-Vertreter gemäss Art. 27 DSGVO in der Europäischen Union zur Seite.

Mit der neuen Datenschutz-Grundverordnung der EU benötigen viele Schweizer Unternehmen, insbesondere Onlineshop-Betreiber, zwingend einen Datenschutz-Vertreter in der EU, wenn sie Waren an Konsumenten in EU-Länder verkaufen, deren Verhalten (mit Cookies oder anderen Marketing-Tools) beobachten oder einen Europäischen Auftragsbearbeiter beauftragen. Der Datenschutz-Vertreter ist Ihre Anlaufstelle für Behörden und betroffene Personen.

[Flyer \(Querformat\)/ Flyer \(Hochformat\)](#)

Unser Angebot

Mit unserem Angebot verfügt Ihr Unternehmen über die **notwendige Datenschutz-Vertretung in der EU** gemäss Art. 27 der Datenschutz-Grundverordnung (DSGVO).

www.eu-datenschutz-vertreter.ch

FSDZ Rechtsanwälte & Notariat AG Zug



Vertretung in der Schweiz



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

**2. Abschnitt:
Datenbearbeitung durch private Verantwortliche mit Sitz oder
Wohnsitz im Ausland**

Art. 14 Vertretung

¹ Private Verantwortliche mit Sitz oder Wohnsitz im Ausland bezeichnen eine Vertretung in der Schweiz, wenn sie Personendaten von Personen in der Schweiz bearbeiten und die Datenbearbeitung die folgenden Voraussetzungen erfüllt:

- a. Die Bearbeitung steht im Zusammenhang mit dem Angebot von Waren und Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz.
- b. Es handelt sich um eine umfangreiche Bearbeitung.
- c. Es handelt sich um eine regelmässige Bearbeitung.
- d. Die Bearbeitung bringt ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich.

² Die Vertretung dient als Anlaufstelle für die betroffenen Personen und den EDÖB.

³ Der Verantwortliche veröffentlicht den Namen und die Adresse der Vertretung.



Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 2 Persönlicher und sachlicher Geltungsbereich

¹ Dieses Gesetz gilt für die Bearbeitung von Personendaten natürlicher Personen durch:

a. private Personen;

b. Bundesorgane.

Unternehmen sind auch private Personen

Kantone erlassen 26 Kantons-DSG

² Es ist nicht anwendbar auf:

- Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;
- Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

Streichung: Schutz der Daten
juristischer Personen

natürlicher Personen



Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

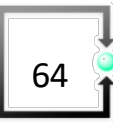
Art. 3 Räumlicher Geltungsbereich

¹ Dieses Gesetz gilt für Sachverhalte, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.

² Für privatrechtliche Ansprüche gilt das Bundesgesetz vom 18. Dezember 1987⁴ über das Internationale Privatrecht. Vorbehalten bleiben zudem die Bestimmungen zum räumlichen Geltungsbereich des Strafgesetzbuchs⁵.

Retorsion zu Art. 3 DSGVO

Personendaten





Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

2. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

a. *Personendaten*: alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen;

c. *besonders schützenswerte Personendaten*:

1. Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten,
2. Daten über die Gesundheit, die Intimsphäre oder die Zugehörigkeit zu einer Rasse oder Ethnie,
3. genetische Daten,
4. biometrische Daten, die eine natürliche Person eindeutig identifizieren,
5. Daten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen,
6. Daten über Massnahmen der sozialen Hilfe;

Neu: Profiling-Daten



2. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

d. *Bearbeiten*: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten;

f. *Profiling*: jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, *Gesundheit*, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

g. *Profiling mit hohem Risiko*: Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;



Verantwortlicher

**Bundesgesetz
über den Datenschutz**
(Datenschutzgesetz, DSG)

2. Kapitel: Allgemeine Bestimmungen
1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

- j. **Verantwortlicher**, private Person oder Bundesorgan, die oder das allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet;

Art. 6 Grundsätze

5 Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Mass-

Auftragsbearbeiter

**Bundesgesetz
über den Datenschutz**
(Datenschutzgesetz, DSG)

2. Kapitel: Allgemeine Bestimmungen
1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

k. *Auftragsbearbeiter*: private Person oder Bundesorgan, die oder das im Auftrag des Verantwortlichen Personendaten bearbeitet.

Auslagerung der Datenbearbeitung (inkl. Cloud-Computing)

Art. 9 **Bearbeitung durch Auftragsbearbeiter**

¹ Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

- a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und
- b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

² Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

³ Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

⁴ Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Art. 28 (1) DSGVO / 9 nDSG

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.

Wer personenbezogene Daten an beizugezogene Service-Provider auslagert, muss einen Auftragsdatenverarbeitungsvertrag (ADV) mit einem Service Level Agreement für TOM's (technische und organisatorische Massnahmen – SLA TOM) abschliessen und vorweisen können.

Art. 28 (2 und 3a-h) DSGVO / 9 nDSG 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.

Ausdrückliche Einwilligung

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

Art. 4 §11 DSGVO / Art. 6 Abs. 6 nDSG

vom 25. September 2020

Art. 6 Grundsätze

⁶ Ist die Einwilligung der betroffenen Person erforderlich, so ist diese Einwilligung nur gültig, wenn sie für eine oder mehrere bestimmte Bearbeitungen nach angemessener Information freiwillig erteilt wird.

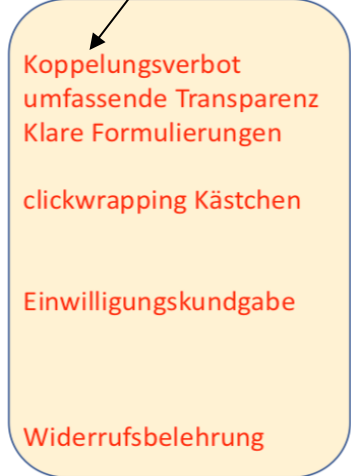
⁷ Die Einwilligung muss ausdrücklich erfolgen für:

- a. die Bearbeitung von besonders schützenswerten Personendaten;
- b. ein Profiling mit hohem Risiko durch eine private Person; oder
- c. ein Profiling durch ein Bundesorgan.

Ausdrückliche Einwilligung

Art. 4 § 11 DSGVO / Art. 6 Abs. 6 nDSG

- **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).



Koppelungsverbot
umfassende Transparenz
Klare Formulierungen

clickwrapping Kästchen

Einwilligungskundgabe

Widerrufsbelehrung



Wir sind für Sie da! Unsere Hilti Stores sind bundesweit für Sie geöffnet **Mehr >**

NEUPRODUKTE & INNOVATIONEN

Entdecken Sie unsere neuesten Hilti Produktinnovationen

[Zu den Neuprodukten >](#)



PROFITIEREN SIE VON PERSONALISIERTEN WEBANGEBOTEN - DURCH DEN GEZIELTEN EINSATZ VON COOKIES

Mit Ihrer Erlaubnis nutzt Hilti Cookies, um die Verwendung unsere Webseiten/Apps einfacher und komfortabler für Sie zu machen.

COOKIE-EINSTELLUNGEN ANNEHMEN

WÄHLEN SIE IHRE INDIVIDUELLEN COOKIE-EINSTELLUNGEN

ANMELDEN / WARENKORB [0]

IHRE COOKIE-EINSTELLUNGEN

Mit Hilfe von Cookies können wir speziell für Sie ausgewählte Inhalte auf unseren Webseiten/Apps bereitstellen.
Mehr erfahren >

Performance Cookies

Performance Cookies helfen uns zu verstehen, wie Sie unsere Webseiten und Apps verwenden. Wir nutzen diese Erkenntnisse, um das Verwenden unserer Webangebote für Sie noch einfacher und komfortabler zu gestalten.

Individualisierte ID ⓘ
 Pseudonymisierte ID ⓘ
 Anonymisierte Cookies ⓘ

Marketing Cookies

Marketing Cookies ermöglichen es uns, für Sie passende Anzeigen auf von Ihnen verwendeten Webseiten und Apps anzuzeigen. In der Regel werden Sie dort auch dann Anzeigen eingeblendet sehen, wenn Sie Marketing Cookies nicht erlauben. In diesem Fall sind die Anzeigen nur allgemeiner Natur. Sie weisen nicht gezielt auf für Sie relevante Angebote hin.

Ja Nein

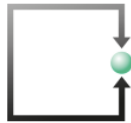
Social Media Cookies

Mit Social Media Cookies ermöglichen Sie uns, für Sie passende Hilti Angebote in Ihren bevorzugten sozialen Netzwerken anzuzeigen. In der Regel werden Sie dort auch dann Anzeigen eingeblendet sehen, wenn Sie Social Media Cookies nicht erlauben. In diesem Fall sind die Anzeigen nur allgemeiner Natur. Sie weisen nicht gezielt auf für Sie relevante Angebote hin.

Ja Nein

SPEICHERN & WEITER

EuGH-Urteil vom 1.10.2019 – Az. C-673/17 (2)



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

[Impressum](#) [Datenschutzbestimmungen](#)

[Profil](#) [Kompetenzen](#) [Team](#) [Aktuell](#) [Publikationen](#) [Referenzen](#) [Kontakt](#)

[« Zurück zur Übersicht](#)

Voreingestellte Einwilligung in Cookies ist unzulässig

Verfasst am 01.10.2019

Der EuGH hat mit einem Urteil entschieden, dass die voreingestellte Einwilligung in Cookies unzulässig ist. Die Internetnutzer müssen demzufolge beim Besuch von Webseiten dem Setzen der Cookies aktiv zustimmen.

[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](#)

FSDZ Rechtsanwälte & Notariat AG Zug



Informationspflichten





Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

3. Kapitel: Pflichten des Verantwortlichen und des Auftragsbearbeiters

Art. 19 Informationspflicht bei der Beschaffung von Personendaten

¹ Der Verantwortliche informiert die betroffene Person angemessen über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

² Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

- a. die Identität und die Kontaktdaten des Verantwortlichen;
- b. den Bearbeitungszweck;
- c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

Anpassung aller Datenschutzbestimmungen auf Webseiten erforderlich

Informationspflichten bei automatisierten Entscheidungen



**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 21 Informationspflicht bei einer automatisierten Einzelentscheidung

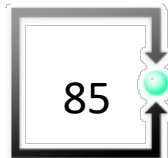
¹ Der Verantwortliche informiert die betroffene Person über eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung beruht und die für sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt (automatisierte Einzelentscheidung).

² Er gibt der betroffenen Person auf Antrag die Möglichkeit, ihren Standpunkt darzulegen. Die betroffene Person kann verlangen, dass die automatisierte Einzelentscheidung von einer natürlichen Person überprüft wird.

³ Die Absätze 1 und 2 gelten nicht, wenn:

- a. die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird; oder**
- b. die betroffene Person ausdrücklich eingewilligt hat, dass die Entscheidung automatisiert erfolgt.**

Bearbeitungsverzeichnis n-DSG





**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 12 Verzeichnis der Bearbeitungstätigkeiten

1 Die Verantwortlichen und Auftragsbearbeiter führen je ein Verzeichnis ihrer Bearbeitungstätigkeiten.

2 Das Verzeichnis des Verantwortlichen enthält mindestens:

- a. die Identität des Verantwortlichen;
- b. den Bearbeitungszweck;
- c. eine Beschreibung der Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
- d. die Kategorien der Empfängerinnen und Empfänger;
- e. wenn möglich die Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
- f. wenn möglich eine allgemeine Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit nach Artikel 8;
- g. falls die Daten ins Ausland bekanntgegeben werden, die Angabe des Staates sowie die Garantien nach Artikel 16 Absatz 2.



Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

vom ...

Art. 4 Bearbeitungsreglement von privaten Personen

¹ Der Verantwortliche und dessen Auftragsbearbeiter müssen ein Reglement für automatisierte Bearbeitungen erstellen, wenn sie:

- a. umfangreich besonders schützenswerte Personendaten bearbeiten; oder
- b. ein Profiling mit hohem Risiko durchführen.

² Das Reglement muss mindestens Angaben enthalten:

- a. zum Bearbeitungszweck;
- b. zu den Kategorien betroffener Personen und der Kategorien bearbeiteter Personendaten;
- c. zur Aufbewahrungsdauer der Personendaten oder die Kriterien zur Festlegung dieser Dauer;
- d. zur internen Organisation;
- e. zur Herkunft der Personendaten und zur Art ihrer Beschaffung;
- f. zu den technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit;
- g. zu den Zugriffsberechtigungen sowie zur Art und zum Umfang der Zugriffe;
- h. zu den Massnahmen, die zur Datenminimierung getroffen werden;
- i. zu den Datenbearbeitungsverfahren, insbesondere den Verfahren bei der Speicherung, Berichtigung, Bekanntgabe, Aufbewahrung, Archivierung, Pseudonymisierung, Anonymisierung und Löschung oder Vernichtung;
- j. zum Verfahren zur Ausübung des Auskunftsrechts und des Rechts auf Datenherausgabe oder -übertragung.

³ Die private Person muss das Reglement regelmässig aktualisieren und der Datenschutzberaterin oder dem Datenschutzberater in einer für diese oder diesen verständlichen Form zur Verfügung stellen.



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

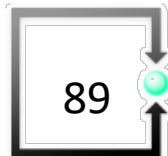
vom 25. September 2020

Art. 12 Abs. 5 nDSG

⁵ Der Bundesrat sieht Ausnahmen für Unternehmen vor, die weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen **und** deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.

Im Bereich HRM dürfte diese Ausnahmebestimmung **NIE** zum Tragen kommen. Also braucht es im Unternehmen diesbezüglich (Mitarbeiterdaten) immer ein **Bearbeitungsverzeichnis**.

Datenschutz-Folgenabschätzung (DSFA) nach n-DSG





Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 22 Datenschutz-Folgenabschätzung

¹ Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein **hohes Risiko** für die **Persönlichkeit oder die Grundrechte der betroffenen Person** mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

² Das **hohe Risiko** ergibt sich, insbesondere bei Verwendung neuer Technologien, aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

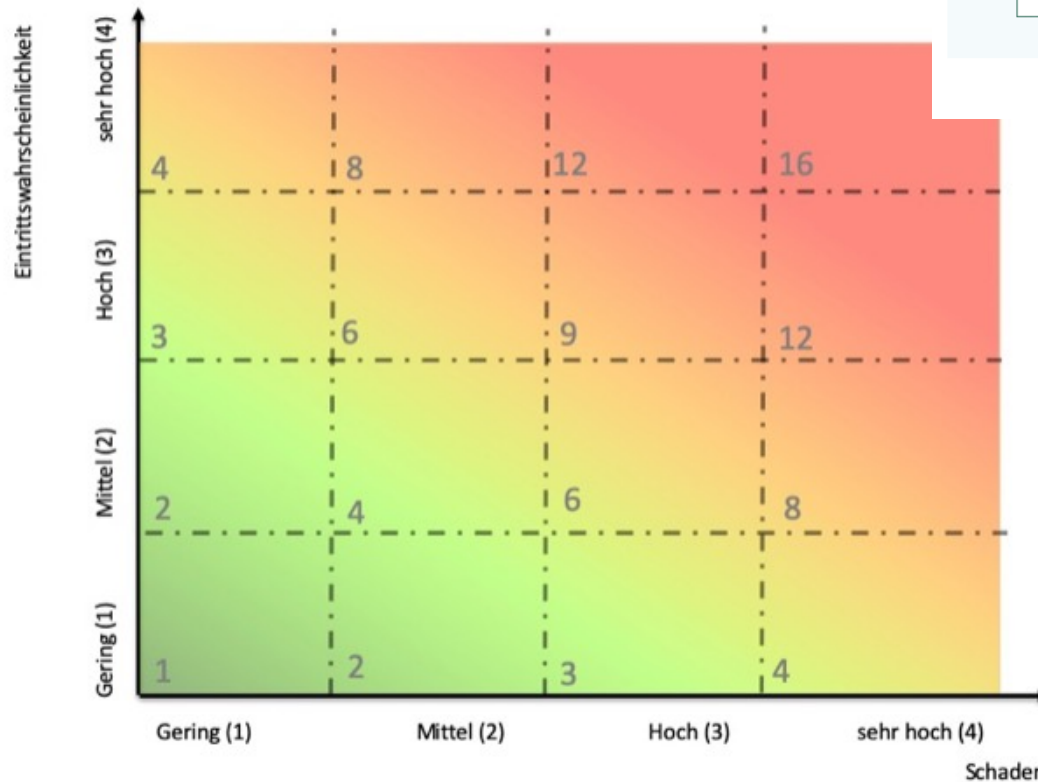
- a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
- b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

³ Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung **eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person** sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

Datenschutz-Folgenabschätzung nach nDSG-CH

Beispiel

Risikomatrix



— NORM [AKTUELL]

ISO/IEC 27005:2018-07

Informationstechnik - IT-Sicherheitsverfahren -
Informationssicherheits-Risikomanagement

Englischer Titel:
Information technology - Security techniques - Information security risk
management

Ausgabedatum:
2018-07

Originalsprachen:
Englisch

Meldepflichten

Data Breach Notifications (nDSG)

Meldung und Benachrichtigung nach nDSG

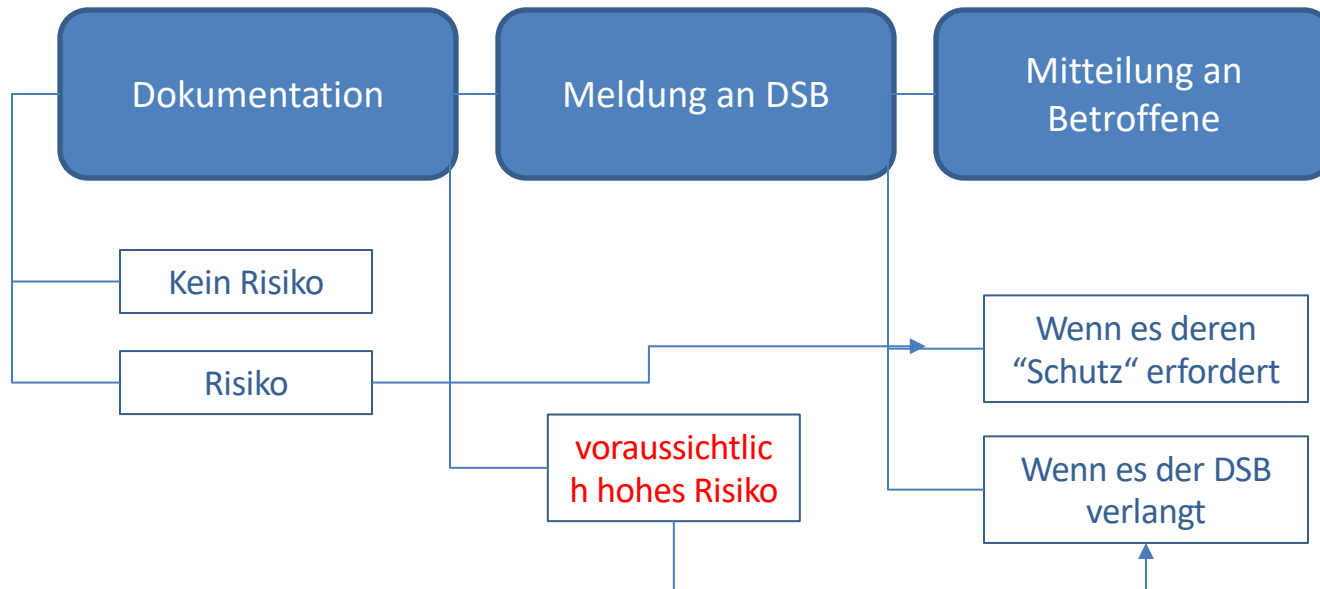
Art. 24 Meldung von Verletzungen der Datensicherheit

1 Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

3 Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit.

4 Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

Meldung und Benachrichtigung nach nDSG



Sanktionen der DSGVO

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.

WhatsApp: Busse von EUR 225 Mio. wegen Verletzung der Informationspflicht

3. September 2021 von David Vasella



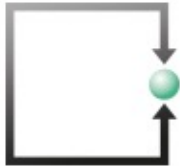
Die irische Datenschutzkommission (Data Protection Commission, DPC) hat am 2. September 2021 den Abschluss einer mehr als zweieinhalb Jahre dauernden Untersuchung bei WhatsApp bekanntgegeben. Gegenstand der Untersuchung war gemäss der [Medienmitteilung der DPC](#), ob WhatsApp die Informationspflichten nach der DSGVO verletzt hat, u.a. auch über den Austausch zwischen WhatsApp und anderen Unternehmen der Facebook-Gruppe. Nicht betroffen war allerdings WhatsApp Business.

Die DPC hat Ende 2020 den mitbetroffenen Aufsichtsbehörden einen Entscheidungsentwurf nach Art. 60 DSGVO vorgelegt. Weil dabei keine Einigkeit gefunden wurde, hat der Europäische Datenschutzausschuss (EDPB) [Ende Juni 2021 die DPC angewiesen](#), die vorgeschlagene Busse zu erhöhen. Infolgedessen verhängte die DPC eine Busse von EUR 225 Mio. gegen WhatsApp, und wies WhatsApp an, die Datenverarbeitung anzupassen.

Der EDPB hielt in seiner Entscheidung u.a. fest, dass **der Verantwortliche für jede einzelne Verarbeitungstätigkeit den Zweck und ggf. die damit verfolgten berechtigten Interessen angeben müsse. Soweit es sich dabei um berechnigte Interessen eines anderen Unternehmens handle, sei auch dieses anzugeben.** Die Datenschutzerklärung und AGB von WhatsApp entsprächen diesen Anforderungen nicht und seien zu wenig klar und spezifisch. Bspw. genüge die Aussage "For providing measurement, analytics, and other business services [...] The legitimate interests we rely on for this processing are: [...] In the interests of businesses and other partners to help them understand their customers and improve their businesses, ...", weil unklar sei, was "other business services" heisse und auch kein berechtigtes Interesse eigens in Bezug auf diesen Zweck genannt werde. Auch bleibe unklar, um welche "businesses or partners" es gehe. Auch "[t]o create, provide, support, and maintain innovative Services and features [...]" sei zu wenig bestimmt.

<https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>

<https://fsdz.ch/aktuell/google-muss-50-millionen-euro-datenschutzstrafe-zahlen/253.blog>



Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | Fax +41 41 727 60 85 |

[i Impressum](#) [🛡️ Datenschutzbestimmungen](#)

[Profil](#) [Kompetenzen](#) - [Team](#) [Aktuell](#) [Publikationen](#) [Referenzen](#) [Kontakt](#)

[« Zurück zur Übersicht](#)

Google muss 50 Millionen Euro Datenschutzstrafe zahlen

Verfasst am 26.01.2019

Die französische Datenschutzbehörde CNIL stellt Verstöße gegen die seit dem 25.5.2018 geltende DSGVO fest und verhängt die bisher höchste Strafe mit Euro 50 Millionen gegen Google.

CNIL bemängelte, die von Google eingeholte Zustimmung zur Anzeige personalisierter Werbung sei nicht gültig, weil die Nutzer nicht ausreichend informiert würden. So sei die Vielfalt der beteiligten Google-Dienste wie YouTube, Google Maps oder der Internet-Suche nicht ersichtlich. Zudem seien Informationen zur Verwendung der erhobenen Daten und dem Speicher-Zeitraum für die Nutzer nicht einfach genug zugänglich, erklärte die Behörde. Sie seien über mehrere Dokumente verteilt und Nutzer müssten sich über mehrere Links und Buttons durchklicken. Zudem seien einige der Informationen unklar formuliert.

Auch CH-Unternehmen betroffen

Informationspflichten aufmerksam wurde und Beschwerde einreichte. Aufgrund der Beschwerde verpflichtete die österreichische Datenschutzbehörde das Schweizer Unternehmen zur nachträglichen Information des Beschwerdeführers und zur Vervollständigung der Information in Ihrer Datenschutzerklärung innert vier Wochen.

Schweizer Hotelbuchungsplattform verletzt die DSGVO-Informationspflicht in Österreich

DIENSTAG, 26. NOVEMBER 2019

Die österreichische Datenschutzbehörde verpflichtet in ihrem Entscheid eine Online-Hotelbuchungsplattform mit Sitz in der Schweiz zur Einhaltung der DSGVO-Informationspflicht. Das Schweizer Unternehmen war den Informationspflichten nur unvollständig nachgekommen und hatte es zudem unterlassen, einen Unionsvertreter zu benennen. Die Anwendbarkeit der DSGVO

Sanktionen

ARTIKEL-29-DATENSCHUTZGRUPPE



17/DE

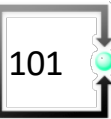
WP 253

**Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der
Verordnung (EU) 2016/679**

angenommen am 3. Oktober 2017

https://www.datenschutzkonferenz-online.de/media/wp/20171003_wp253.pdf

Sanktionen im Schweizerischen Bundes-Datenschutzgesetz (inkl. kantonale DSG)





**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

8. Kapitel: Strafbestimmungen

Art. 60

Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

1 Mit Busse bis zu 250 000 Franken werden private Personen auf Antrag bestraft:

- a. die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;
- b. die es vorsätzlich unterlassen:
 1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder
 2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

2 Mit Busse bis zu 250 000 Franken werden private Personen bestraft, die unter Verstoß gegen Artikel 49 Absatz 3 dem EDOB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.



**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 61 Verletzung von Sorgfaltspflichten

Mit Busse bis zu 250 000 Franken werden **private Personen** auf Antrag bestraft, die vorsätzlich:

- a. unter Verstoss gegen Artikel 16 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 17 erfüllt sind, Personendaten ins Ausland bekanntgeben;
- b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 9 Absätze 1 und 2 erfüllt sind;
- c. die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach Artikel 8 Absatz 3 erlassen hat, nicht einhalten.



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 62 Verletzung der beruflichen Schweigepflicht

1 Wer geheime Personendaten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder seines Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wird auf Antrag mit Busse bis zu 250 000 Franken bestraft.

2 Gleich wird bestraft, wer vorsätzlich geheime Personendaten offenbart, von denen sie oder er bei der Tätigkeit für eine geheimhaltungspflichtige Person oder während der Ausbildung bei dieser Kenntnis erlangt hat.

3 Das Offenbaren geheimer Personendaten ist auch nach Beendigung der Berufsausübung oder der Ausbildung strafbar.



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 63 Missachten von Verfügungen

Mit Busse bis zu 250 000 Franken werden **private Personen** bestraft, die einer Verfügung des EDOB oder einem Entscheid der Rechtsmittelinstanzen, die oder der unter Hinweis auf die Strafdrohung dieses Artikels ergangen ist, vorsätzlich nicht Folge leisten.



**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 65 Zuständigkeit

¹ Die Verfolgung und die Beurteilung strafbarer Handlungen obliegen den Kantonen.

² Der EDÖB kann bei der zuständigen Strafverfolgungsbehörde Anzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen.

Art. 66 Verfolgungsverjährung

Die Strafverfolgung verjährt nach fünf Jahren.

Grundsätze der IT-Sicherheit im neuen Datenschutzrecht



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

2. Kapitel: Allgemeine Bestimmungen
1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

- h. *Verletzung der Datensicherheit*: eine Verletzung der Sicherheit, die dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden;



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 7 **Datenschutz durch Technik und datenschutzfreundliche
Voreinstellungen**

1 Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 6. Er berücksichtigt dies ab der Planung.

2 Die technischen und organisatorischen Massnahmen müssen insbesondere dem **Stand der Technik**, der **Art und dem Umfang der Datenbearbeitung** sowie dem **Risiko**, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

Art. 8 **Datensicherheit**

1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

2 Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

3 Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

Datenbearbeitungsvertrag mit Auftragsbearbeiter (ADV)



Ablauf der Referendumsfrist: 14. Januar 2021

**Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)**

vom 25. September 2020

**Vertrags- und Auditpflichten für
Verantwortlichen**

Art. 9 **Bearbeitung durch Auftragsbearbeiter**

¹ Die Bearbeitung von Personendaten kann vertraglich oder durch die Gesetzgebung einem Auftragsbearbeiter übertragen werden, wenn:

- a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und
- b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

² Der Verantwortliche muss sich insbesondere vergewissern, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten.

³ Der Auftragsbearbeiter darf die Bearbeitung nur mit vorgängiger Genehmigung des Verantwortlichen einem Dritten übertragen.

**Verordnung
zum Bundesgesetz über den Datenschutz
(VDSG)**

vom ...

Schutzziele

Art. 2 Schutzziele

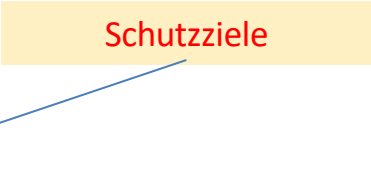
Soweit angemessen, müssen die Massnahmen zur Gewährleistung der Datensicherheit folgende Schutzziele erreichen:

- a. **Zugriffskontrolle:** Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.
- b. **Zugangskontrolle:** Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.
- c. **Datenträgerkontrolle:** Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht.
- d. **Speicherkontrolle:** Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert.
- e. **Benutzerkontrolle:** Die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert.
- f. **Transportkontrolle:** Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Verordnung
zum Bundesgesetz über den Datenschutz
(VDSG)

vom ...

Schutzziele



- g. Eingabekontrolle:** In automatisierten Systemen kann überprüft werden, welche Personendaten zu welcher Zeit und von welcher Person eingegeben oder verändert wurden.
- h. Bekanntgabekontrolle:** Es kann überprüft werden, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekannt gegeben wurden.
- i. Wiederherstellung:** Die Verfügbarkeit der Personendaten und der Zugang zu ihnen kann bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden.
- j.** Es wird gewährleistet, dass alle Funktionen des Systems zur Verfügung stehen (**Verfügbarkeit**), auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit**) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**).
- k. Erkennung:** Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.

Aktuell	Datenschutz	Öffentlichkeitsprinzip	Dokumentation	Der EDÖB	
---------	-------------	------------------------	---------------	----------	--

[Startseite](#) > [Datenschutz](#) > [Dokumentation](#) > [Leitfäden](#) > Technische und organisatorische Massnahmen

[← Dokumentation](#)


Leitfäden

Wahlen und Abstimmungen

Rechte der betroffenen Personen

Technische und organisatorische Massnahmen des Datenschutzes



 [Leitfaden zu den technischen und organisatorischen Massnahmen zum
Datenschutz \(PDF, 1 MB, 21.08.2015\)](#)

<https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html>

Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes

August 2015



Wird auf den 1.9.2023
überarbeitet werden

Inhaltsverzeichnis

Einleitung.....	3
Begriffe.....	3
Daten-/Informationssicherheit.....	3
Datenschutz.....	3
Informationsschutz.....	3
Personendaten.....	4
Datensammlung.....	4
Zuständigkeiten.....	5
Gesetzliche Grundlagen.....	5
Technische und organisatorische Massnahmen.....	5
Inhalt des Leitfadens.....	6
Schwerpunkt A. Zugang zu den Daten.....	7
A.1 Sicherheit der Räumlichkeiten.....	8
A.2 Sicherheit der Serverräume.....	9
A.3 Sicherheit des Arbeitsplatzes.....	9
A.4 Identifizierung und Authentifizierung.....	10
A.5 Zugang zu den Daten.....	11
A.6 Zugang von ausserhalb der Organisation.....	12
Schwerpunkt B. Lebenszyklus von Daten.....	13
B.1 Datenerfassung.....	14
B.2 Protokollierung.....	14
B.3 Pseudonymisierung und Anonymisierung.....	15
B.4 Verschlüsselung.....	17
B.5 Sicherheit der Datenträger.....	17
B.6 Datensicherung.....	18
B.7 Datenvernichtung.....	18
B.8 Auslagerung von Arbeiten (Bearbeitung durch Dritte).....	19
B.9 Sicherheit und Schutz.....	19
Schwerpunkt C. Datenaustausch.....	21
C.1 Netzsicherheit.....	22
C.2 Verschlüsselung von Mitteilungen.....	22
C.3 Unterzeichnen von Mitteilungen.....	24
C.4 Übergabe von Datenträgern.....	26
C.5 Protokollierung des Datenaustauschs.....	26
Schwerpunkt D. Auskunftsrecht.....	27
D.1 Recht der betroffenen Personen.....	27
D.2 Reproduzierbarkeit der Verfahren.....	28
Hilfsmittel.....	29
Das Bearbeitungsreglement.....	29
Inhalt des Reglements.....	29
Schlussbemerkung.....	30

Selbstdeklaration des SaaS-Anbieters zum Rahmenvertrag für die Bereitstellung und den Betrieb von ärztlichen Fachapplikationen aus der Cloud

4. Organisatorische Massnahmen

Deklaration	Antwort Anbieter	Beilagen / Ergänzung / Bemerkungen / Links
4.1. Der Anbieter stellt dem Kunden eine umfassende Dokumentation zu allen angebotenen SaaS-Dienstleistungen zur Verfügung, welche alle enthaltenen Funktionen beschreibt und umfassend über		

34 Massnahmenvorschläge

5. Technische Massnahmen

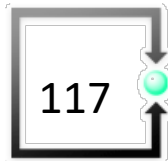
Die nachfolgenden Massnahmen sind insbesondere dem Leitfaden des Eidgenössischen Datenschutzbeauftragten für die Bearbeitung von Personendaten im medizinischen Bereich vom Juli 2002 sowie den Minimalanforderungen der FMH für IT-Grundschutz für Praxisärztinnen und Praxisärzte (<https://www.fmh.ch/dienstleistungen/e-health/it-grundschutz.cfm>) entnommen.

Deklaration	Antwort Anbieter	Beilagen / Ergänzung / Bemerkungen / Links
5.1. Erlässt der Anbieter zuhanden des Kunden <u>konkrete</u> Sicherheitsvorgaben, welche dieser umzusetzen und einzuhalten hat? Wenn ja, welche? Kann er dafür die entsprechenden Vorhaben		

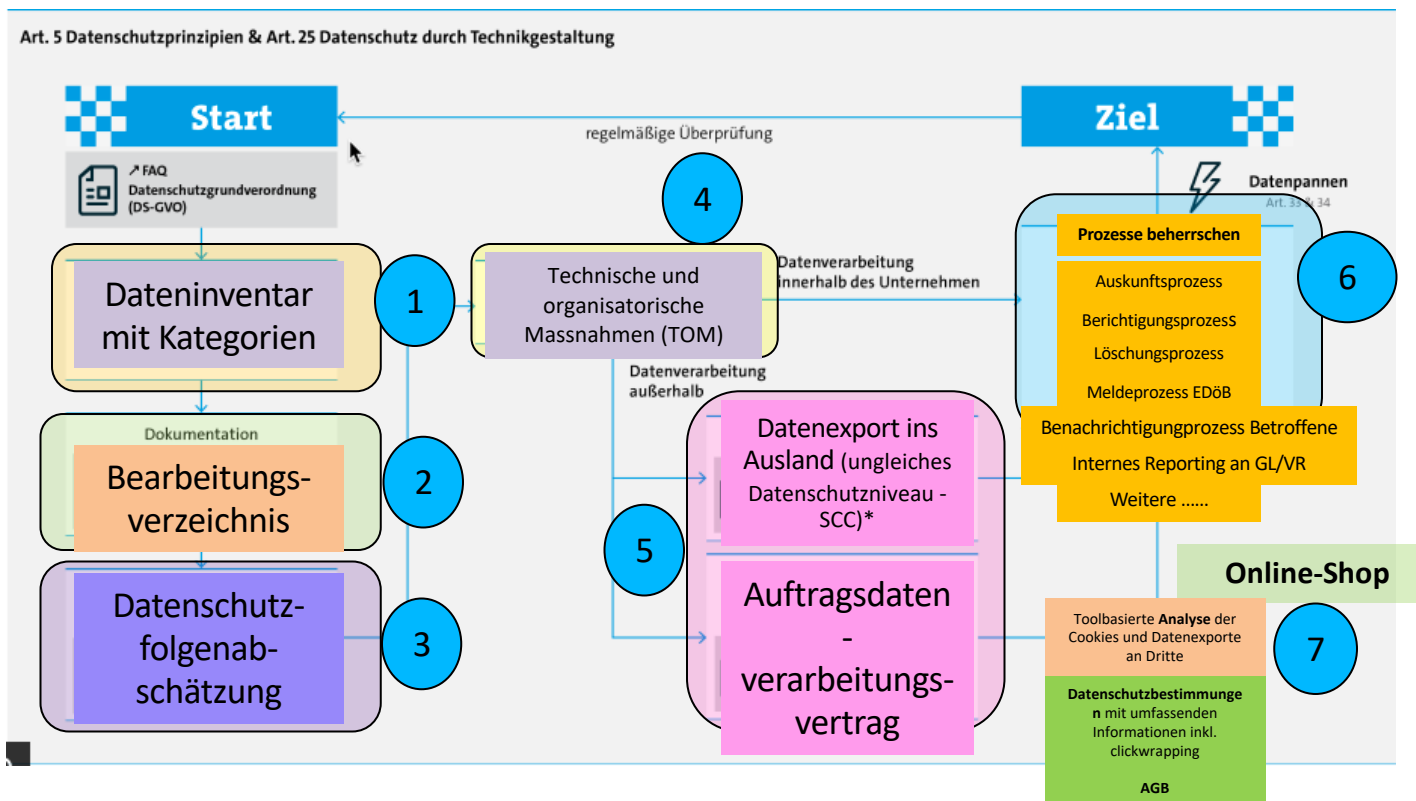
20 Massnahmenvorschläge

https://www.fsdz.ch/file-docs/selbstdeklaration_zum_rahmenvertrag_cloudservices_fmh_-_finale_publicationsversion_2-00_-_14-01-2020.pdf

Umsetzungsmassnahmen zum neuen Datenschutzgesetz der Schweiz



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)

FSDZ Rechtsanwälte & Notariat AG Zug

* <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html#-291511647>

Handlungsbedarf unter neuem CH-DSG

1. **Inventar der Personendaten in Applikationen** (interne und externe) und **Ablagen** erstellen
2. **Datenschutzerklärungen auf den neuesten Stand bringen**; prüfen ob alle Fälle abgedeckt sind, wo das Unternehmen Personendaten beschafft und bearbeitet.
3. **Verzeichnis der Bearbeitungstätigkeiten** erstellen (Wer macht was mit welchen Daten wie -> Prozesslandkarte und Prozessbeschreibung; Ausnahmebestimmungen; **Empfehlung trotzdem erstellen**)
4. **Vertrag zu Auftragsdatenverarbeitungen** (externe) identifizieren und Verträge (ADDV) mit Service-Providern anpassen.
5. Auslandtransfers identifizieren und offenlegen (DSE)
6. **Prozess für Datenschutz-Folgeabschätzung** einführen
7. **Datenschutz-Folgeabschätzung** durchführen
8. **Verzeichnis Technische und Organisatorische Massnahmen** (intern und extern) festlegen (allenfalls in neue SLA des ADVV mit Providern einbinden)

Muss-Dokument

Muss-Dokument

Muss-Dokument

Muss-Dokument

Handlungsbedarf unter neuem CH-DSG

10. **Prozesse zur Meldung und Benachrichtigung** von Verletzungen des Datenschutzes und der Datensicherheit einführen
11. Vorgaben und **Prozesse für alle Ersuchen von Betroffenen** erstellen oder anpassen.
11. Automatisierte Einzelentscheide im Unternehmen identifizieren und – sofern vorhanden – neu regeln.
12. periodische **Awareness-Schulung** durchführen, dokumentieren und **Weisungen** an Mitarbeiter anpassen sowie **allenfalls interne Audits** vorsehen und dokumentieren (**Nachweise sicherstellen**).
13. **Datenschutzerklärungen** (auf Websites, Onlineshops etc.) anpassen. Muss-Dokument
14. Online-Shops **umfassende Informationspflichten** bezüglich Einsatz von Cookies, Profiling-Tools, Targeting-Tools oder Einsatz weiterer Erfassungswerkzeuge prüfen und Datenschutzbestimmungen anpassen. Muss-Anforderung
15. **Einwilligungen des Benutzers durch „clickwrapping“** einholen (Modell der diversifizierten Zustimmung vorsehen) Muss-Anforderung

The Roadmap to Compliance

Sie müssen das neue Datenschutzrecht
spätestens mit Inkrafttreten
des neuen CH-Datenschutzgesetzes
sowieso umsetzen.

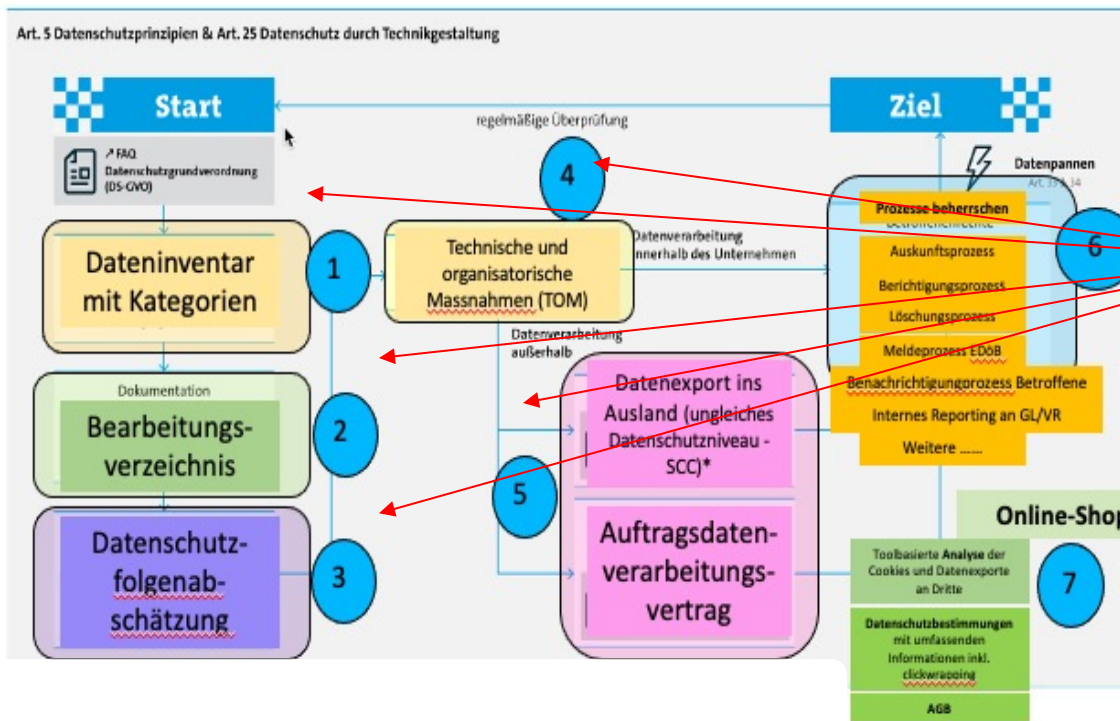
Fangen Sie unbedingt jetzt damit an.

The Roadmap to Compliance

Sie brauchen ein **Frühwarnsystem mit Beobachtungsturm** und ein neues Risikoverständnis bezüglich Datenschutz und Datensicherheit

- Compliance-Verantwortung (VR & GL: DP-Policy)
- DS-Beauftragter oder DS-Verantwortlicher
- Berücksichtigung im Rahmen des IKS
- Kontinuierliche Verbesserung und Anpassung
- periodische Risikoüberprüfung
- Nachweisdokumentationen

Unsere Unterstützungsleistungen



Team erarbeitet Entwürfe nach Projektplan

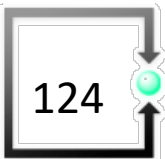
Wir **reviewen** Ihre Entwürfe und geben Verbesserungs-Feedback

Team passt Entwürfe an und finalisiert diese.

Unternehmen schult seine Mitarbeitenden auf den 1.9.2023

Fazit:

Verantwortung und Sorgfaltspflichten der
Führungskräfte hinsichtlich der Digitalisierung im
Unternehmen



- Der Umgang mit allen digitalen Risiken im Unternehmen gehört in den Aufgabenbereich des VR und der GL (Führungsaufgabe: Art. 716 Abs. 5 OR)
- Rasanter technologischer Wandel zwingt zu periodischer, mindestens einmal jährlicher Überprüfung der veranlassten technischen und organisatorischen, prozessualen und personellen sowie finanziellen Massnahmen zur Vermeidung von digitalen Risiken
- **Die Beweislast für die Erfüllung der Sorgfaltspflichten liegt bei GL und VR**
- Die Haftung dehnt sich in den persönlichen Bereich aller Mitgliedern der GL und VR aus (Grobfahrlässigkeit).

- **Umsetzung der neuen Datensicherheitsvorgaben gemäss CH-DSG**
 - Dateninventar, Bearbeitungsverzeichnis, Datenschutzfolgeabschätzung, techn. und organ. Massnahmen (TOM's), Verträge mit Datenverarbeitern
- **Prozessbeschreibungen** für
 - Wahrung der Rechte der Betroffenen (Kunden, Lieferanten etc.)
 - Meldepflichten an Datenschutzbehörde
 - Benachrichtigungen an Betroffene
- **Jährliche Überprüfung der Cyberrisiko-Situation und der TOM's**
 - GAP-Analyse in GL vorbereiten und mit VR abstimmen
 - Standard-Traktandum 1x jährlich Analyse und Beschlüsse protokollieren
- **Awareness-Schulungen der Mitarbeitenden (Nachweise)**

Besten Dank

Lukas Fässler

Rechtsanwalt & Informatikexperte

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76B

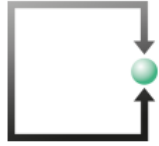
CH-6340 Baar

Tel. +41 +41 727 60 80

www.fsdz.ch

faessler@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

Impressum Datenschutzbestimmungen

Profil Kompetenzen - Team Aktuell Publikationen Referenzen Kontakt

Aktuelles aus unserer Kanzlei.

Alle Intern Publikationen Veranstaltungen

CAS Information-Security und Risk-Management

Verfasst am 29.05.2019

Fachhochschule Nordwest-Schweiz, FHNW in Basel

Rechtsanwalt Lukas Fässler unterrichtet an der FHNW in Basel. In diesem Kursmodul werden aus der Sicht IT-Sicherheit und IT-Riskmanagement folgende Aspekte beleuchtet:

- Grundsätze der Unternehmensführung
 - Corporate Governance und Compliance
 - Grundsätze von Datenschutz und neues Datenschutzrecht (DSGVO und E-DSG Schweiz)
 - Grundsätze von IT-Sicherheit
 - Schadensbegrenzung und Abwägung
- »Weiterlesen

Datenschutz und Datensicherheit in der Arztpraxis

Verfasst am 16.05.2019

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

Rechtsanwältin und Notarin
lic. iur. Carmen de la Cruz Böhlinger
Telefon +41 41 727 60 80
sekretariat@fsdz.ch

Dienstleistungen / EU Datenschutz-Vertreter

Datenschutz-Vertreter in der Europäischen Union EU

Mit der neuen Datenschutz-Grundverordnung der EU benötigen Schweizer Onlineshop-Betreiber zwingend einen Datenschutz-Vertreter in der EU, wenn sie Waren in EU-Länder verkaufen. Der Vertreter muss in dem Land niedergelassen sein, in dem der Käufer wohnt und in das die Waren exportiert werden.

e-comtrust international vermittelt Schweizer Onlineshop - Betreibern einen solchen Datenschutz-Vertreter.

Erfahren Sie mehr dazu und bestellen Sie bei e-comtrust international Ihren Datenschutzvertreter.

- Flyer zur neuen Pflicht für CH-Online-Shopbetreiber
- Formular für die Bestellung EU-Datenschutzvertreter

 **Jetzt beraten lassen**
+41 41 727 00 70

 **Webshop
zertifizieren**
Jetzt mehr erfahren

Aktuell bei e-comtrust

Domaininhaber haftet für Wettbewerbsverstoss des Pächters

01.03.2018 - Der Pächter einer Domain machte mit einem kostenlosen FitBand Werbung für seine Nahrungsergänzungsprodukt. Dies wurde dem Domaininhaber zum rechtlichen Verhängnis.

[» zum kompletten Artikel](#)

Besten Dank

Lukas Fässler

Rechtsanwalt & Informatikexperte

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76B

CH-6340 Baar

Tel. +41 +41 727 60 80

www.fsdz.ch

faessler@fsdz.ch

