Fachhochschule Nordwestschweiz
Hochschule für Wirtschaft

Seminar Neues Datenschutzrecht (nCH-DSG und DSGVO)

Daten schützen und digitale Verantwortung rechtskonform umsetzen.

Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

www.fsdz.ch

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

Impressum Datenschutzbestimmungen

Hinweis schliessen

Umsetzung der DSGVO

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

Lukas Fässler

Rechtsanwalt und Informatikexperte, Certified Software Asset Manager IAITAM Inc.

faessler@fsdz.ch
+41 41 727 60 80
+41 79 209 24 32

Profil

1975 – 1980
Studium an der Universität Fribourg/CH

1982
Anwaltspatent des Kantons Luzern

1982 – 1984
Gerichtsschreiber am Amtsgericht Hochdorf

1984 - 1987
Gerichtsschreiber am Verwaltungsgericht Luzern

1987 - 1992
EDV-Beauftragter im Gerichtswesen Kanton Luzern

1992 - 1997
Informatikchef des Kantons Luzern

1997
Selbständiger Spezialanwalt seit September 1997

1999 - 2000
Universität Zürich, Nachdiplomstudium, Internationales Wirtschaftsrecht (Spezialisierungskurs Immaterialgüterrecht, Technologie- und Informationsrecht)

2017
"Certified Software Asset Manager IAITAM Inc." bei der International Association of Information Techology Asset Managers Inc. in Amerika

Verwaltungsratsmandate

- Verwaltungsratspräsident FSDZ Rechtsanwälte & Notariat AG Baar
- Verwaltungsratspräsident e-comtrust international AG, Baar mit Zweigniederlassung Bremen
- Verwaltungsratspräsident AR Informatik AG
- Verwaltungsrat Health Info Net AG (HIN)
- Vizepräsident Verwaltungsrat ILZ OW/NW
- Verwaltungsrat Eisenbahnbetriebslabor Schweiz AG

- Präsident Verein Schweizerische Städte- und Gemeinde-Informatik SSGI
- Präsident Verein EWML

Dozententätigkeiten

- **Universität Basel:**
  - Master of Marketing Management, eCommerce-Recht EU und CH
- **Universität Bern/Lausanne:**
  - Master of Advanced Studies for Archival an Information Management

- **Fachhochschule Nordwestschweiz in Basel:**
  - CAS eCommerce und Online-Marketing
  - CAS Information Security & Risk Management
  - CAS IT Service Management & IT Controlling
  - CAS Operational Risk Management
  - Seminar Digital Leadership
  - Praxis-Seminar DSGVO und CH E-DSG
  - Seminar öffentliches Beschaffungsrecht

- **Fachhochschule Nordwestschweiz in Olten:**
  - CAS Data und Information Management

Tag 1 und 2

Seminar Neues Datenschutzrecht (nCH-DSG und EU-DSGVO)

Tag 1

Seminareinführung
Dr. Bettina Schneider 09.00-09.30

- Big Picture. Einführung zum Seminar
  Warm Up & Kennenlernen

Neues Schweizer DSG und die europäische DSGVO
Lukas Fässler 09.30-12.15

- Neues Schweizer DSG (nCH-DSG)
- Verantwortungsträger im Unternehmen, NPO, Organisationen und öffentlichen Verwaltungen
- Compliance-Vorgaben im Allgemeinen
- Grundlagen des Datenschutzes und der IT-Sicherheit

Mittagspause 12.15-13.15

- Grundprinzipien des neuen Schweizer Datenschutzgesetzes nCH-DSG
- Grundprinzipien der europäischen DSGVO
- Territorialer Geltungsbereich der DSGVO
- Safe Harbor Ade – neue Anforderungen an Data transborder Agreements bis 17.00

Tag 2

Schweizer DSG: Entwicklung eines Datenschutzkonzeptes
Lukas Fässler

- Warm up 09.00-12.15
- Datenschutz:
  Die neuen Instrumente des
- Rechtssicherheit:
  The Roadmap to Compliance
- Datensicherheitskonzept als Bestandteil des Datenschutzes – Prinzipien

Mittagspause 12.15-13.15

- Praxisaufgabe: (Bettina Schneider) 13.15-14.00
  Verarbeitungsverzeichnis
  (Einführung & praktisches Beispiel)
- Praxisaufgabe (Esther Zaugg) 14.15-15.40
  Datenschutzfolgeabschätzung
  (Einführung & Tool)
- Praxisaufgabe: (Lukas Fässler) 16.00-16.45
  Erarbeitung der Data Protection Policy
  (Stufe VR)
- Aufgabenverteilung für Tag 3 bis 17.00

Homework bis zum letzten Kurstag

- Entwurf **Data Protection Policy** fertigstellen und Präsentation vorbereiten
- **Datenschutz-Folge-abschätzung** (DSFA) fertigstellen und Präsentation vorbereiten
- **Verzeichnis von Verarbeitungstätigkeiten** fertigstellen und Präsentation vorbereiten

Teil 1

Verantwortungsträger im Unternehmen und in öffentlichen Verwaltungen

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 Unternehme 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 berechtigte 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

Wenn in Europa DataCenters brennen, kommen Fragen der Business 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

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-einzige-zeitungspapierfabrik-der-schweiz-lahm-mit-folgen

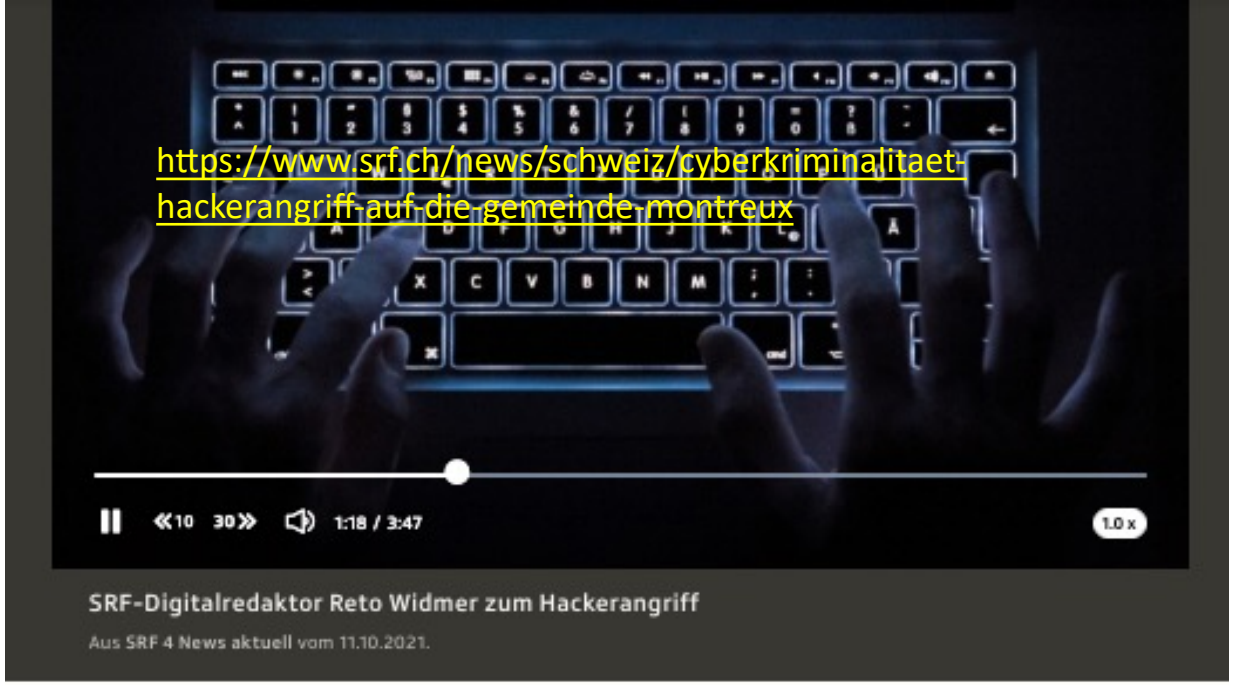
Hackerangriff auf die Rothenburger Auto AG Group

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)



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

News > Schweiz >

Cyberkriminalität

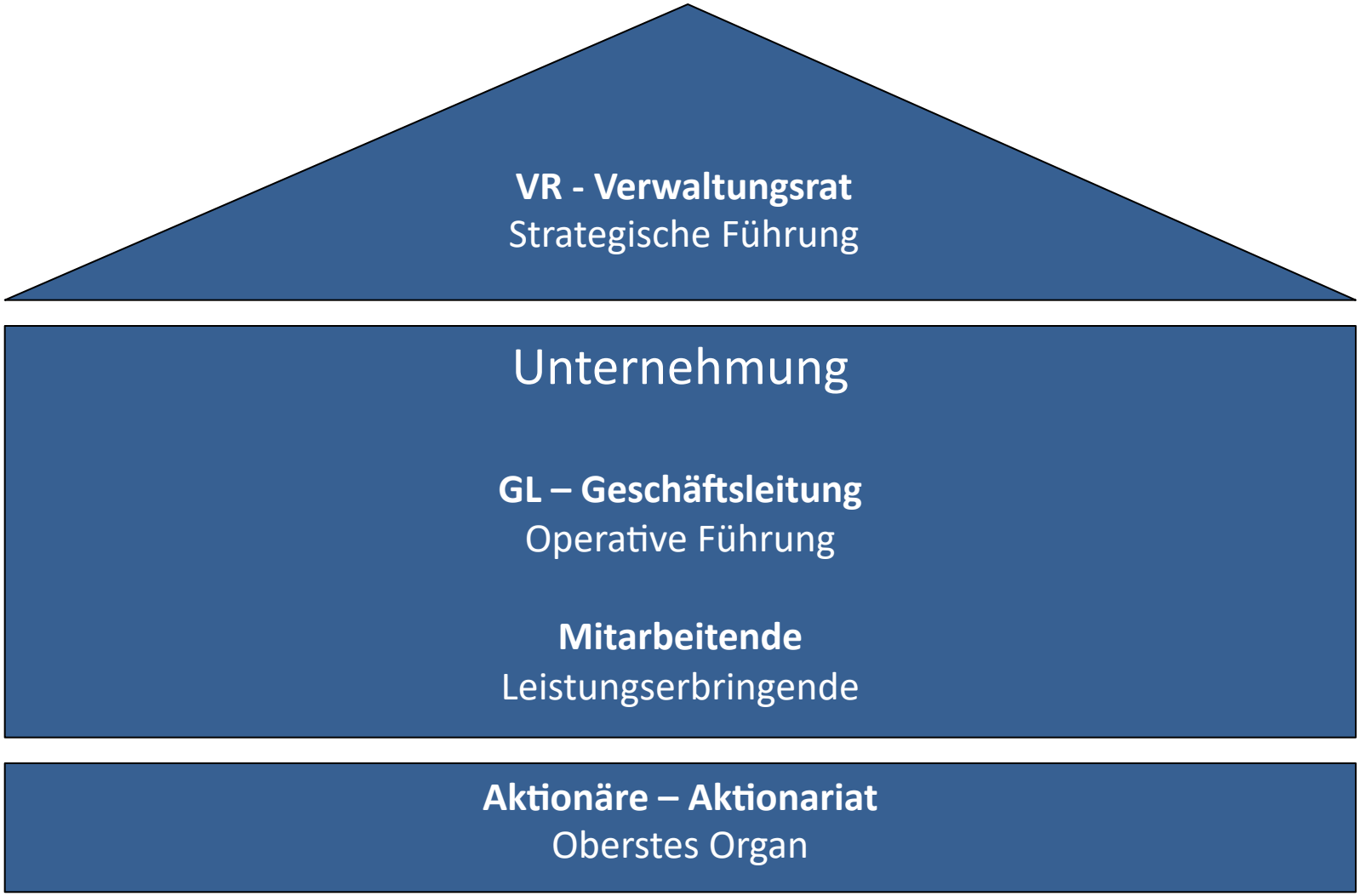
Hackerangriff auf die Gemeinde Montreux

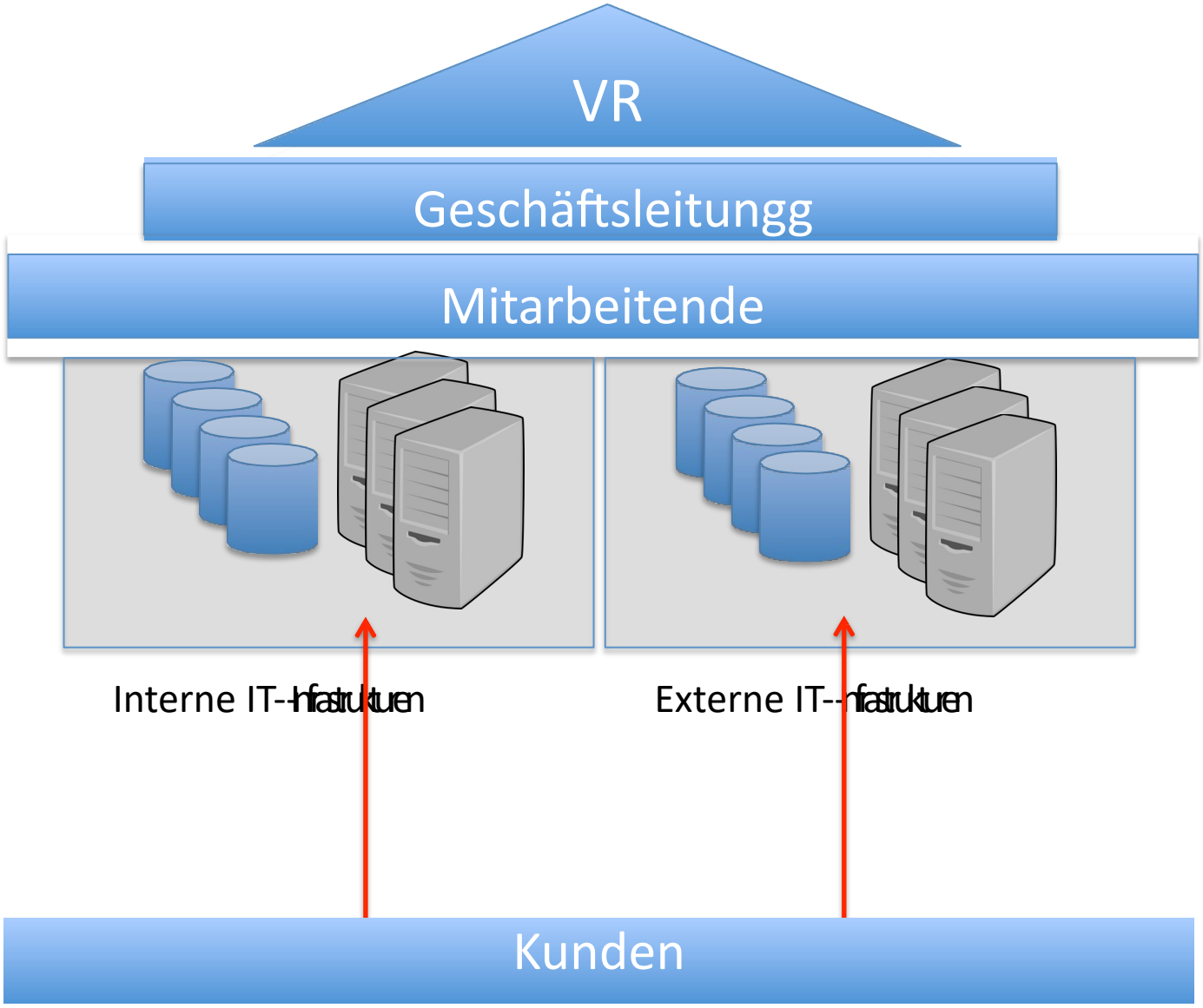
Montag, 11.10.2021, 08:17 Uhr
Aktualisiert um 11:33 Uhr

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.

Das Unternehmen

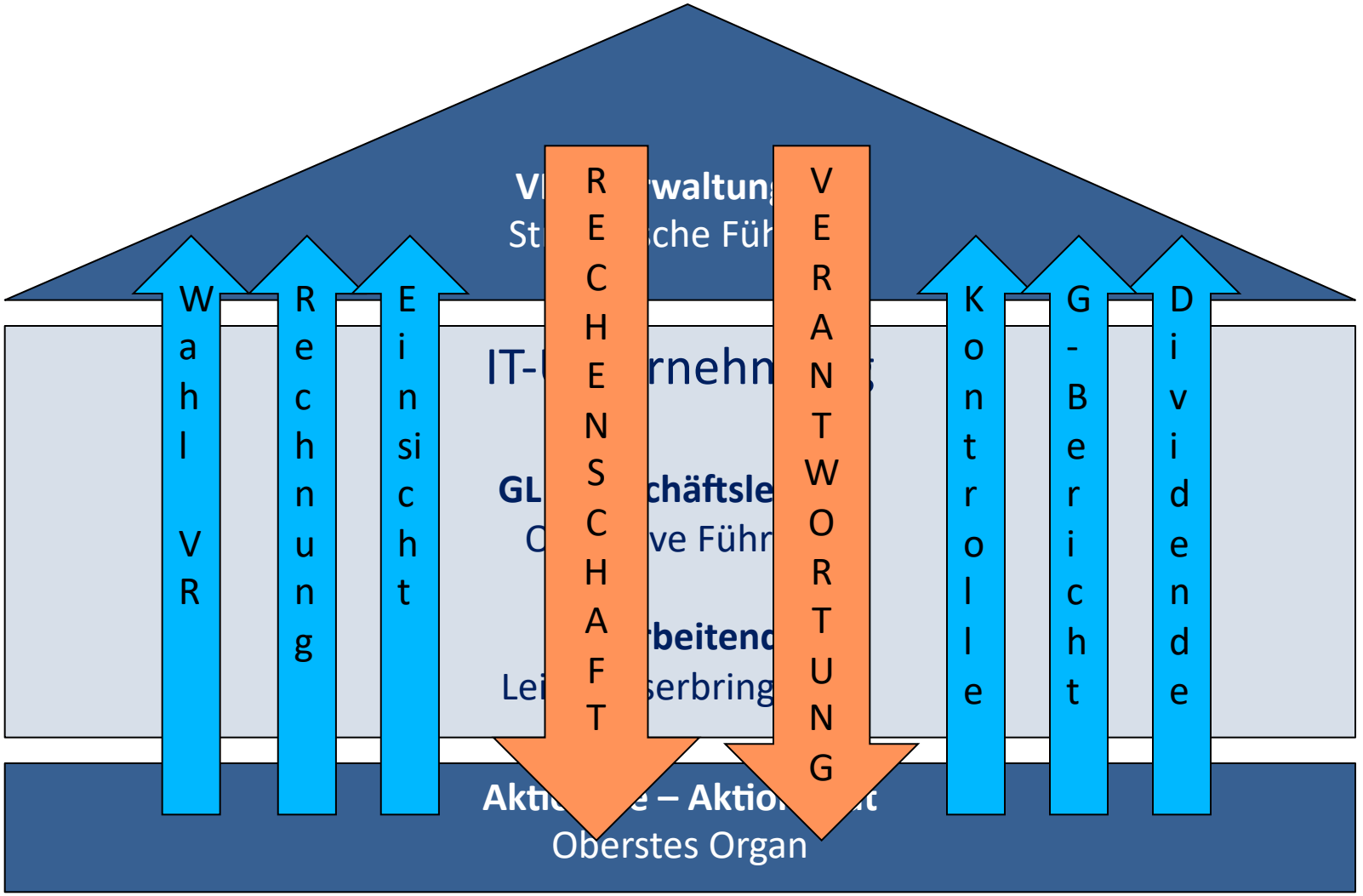

VR - Verwaltungsrat
Strategische Führung
Unternehmung
GL – Geschäftsleitung
Operative Führung
Mitarbeitende
Leistungserbringende
Aktionäre – Aktionariat
Oberstes Organ


VR
Geschäftsleitungg
Mitarbeitende
Interne IT-Infrastrukturen
Externe IT-Infrastrukturen
Kunden

Die gesetzlichen Grundlagen zur Unternehmensführung

Die Generalversammlung der Aktionäre

Aktionäre – Aktionariat
Oberstes Organ


Wahl VR
Rechnung
Einsicht
RECHENSCHAFT
VERANTWORTUNG
Kontrolle
G-Bericht
Dividende
Oberstes Organ

Dritter Abschnitt: Organisation der Aktiengesellschaft

A. Die Generalversammlung

Art. 698

I. Befugnisse

[1] Oberstes Organ der Aktiengesellschaft ist die Generalversammlung der Aktionäre.

[2] Ihr stehen folgende unübertragbare Befugnisse zu:

1. die Festsetzung und Änderung der Statuten;
2. die Wahl der Mitglieder des Verwaltungsrates und der Revisionsstelle;
3. [392] die Genehmigung des Lageberichts und der Konzernrechnung;
4. die Genehmigung der Jahresrechnung sowie die Beschlussfassung über die Verwendung des Bilanzgewinnes, insbesondere die Festsetzung der Dividende und der Tantieme;
5. die Entlastung der Mitglieder des Verwaltungsrates;
6. die Beschlussfassung über die Gegenstände, die der Generalversammlung durch das Gesetz oder die Statuten vorbehalten sind.[393]

Aktionäre – Aktionariat
Oberstes Organ

Zweiter Abschnitt: Rechte und Pflichten der Aktionäre

Art. 660[324]

A. Recht auf Gewinn- und Liquidationsanteil

I. Im Allgemeinen

[1] Jeder Aktionär hat Anspruch auf einen verhältnismässigen Anteil am Bilanzgewinn, soweit dieser nach dem Gesetz oder den Statuten zur Verteilung unter die Aktionäre bestimmt ist.

[2] Bei Auflösung der Gesellschaft hat der Aktionär, soweit die Statuten über die Verwendung des Vermögens der aufgelösten Gesellschaft nichts anderes bestimmen, das Recht auf einen verhältnismässigen Anteil am Ergebnis der Liquidation.

Aktionäre – Aktionariat
Oberstes Organ

Der Verwaltungsrat
Oberste strategische Führung

Teil 2

Compliance-Vorgaben im Allgemeinen

Allgemeine gesetzliche Grundlagen

VR - Verwaltungsrat
Strategische Führung

Art. 716*a*[430]

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[431] 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.

B. Der Verwaltungsrat[414]

5. die Oberaufsicht 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 Verwaltungsrat[414]

Art. 717[433]

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, Geschäftsführung und Liquidation

Art. 754[488]

[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

Urteilskopf

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 CORBOZ, 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**).

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

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

Beweislastumkehr

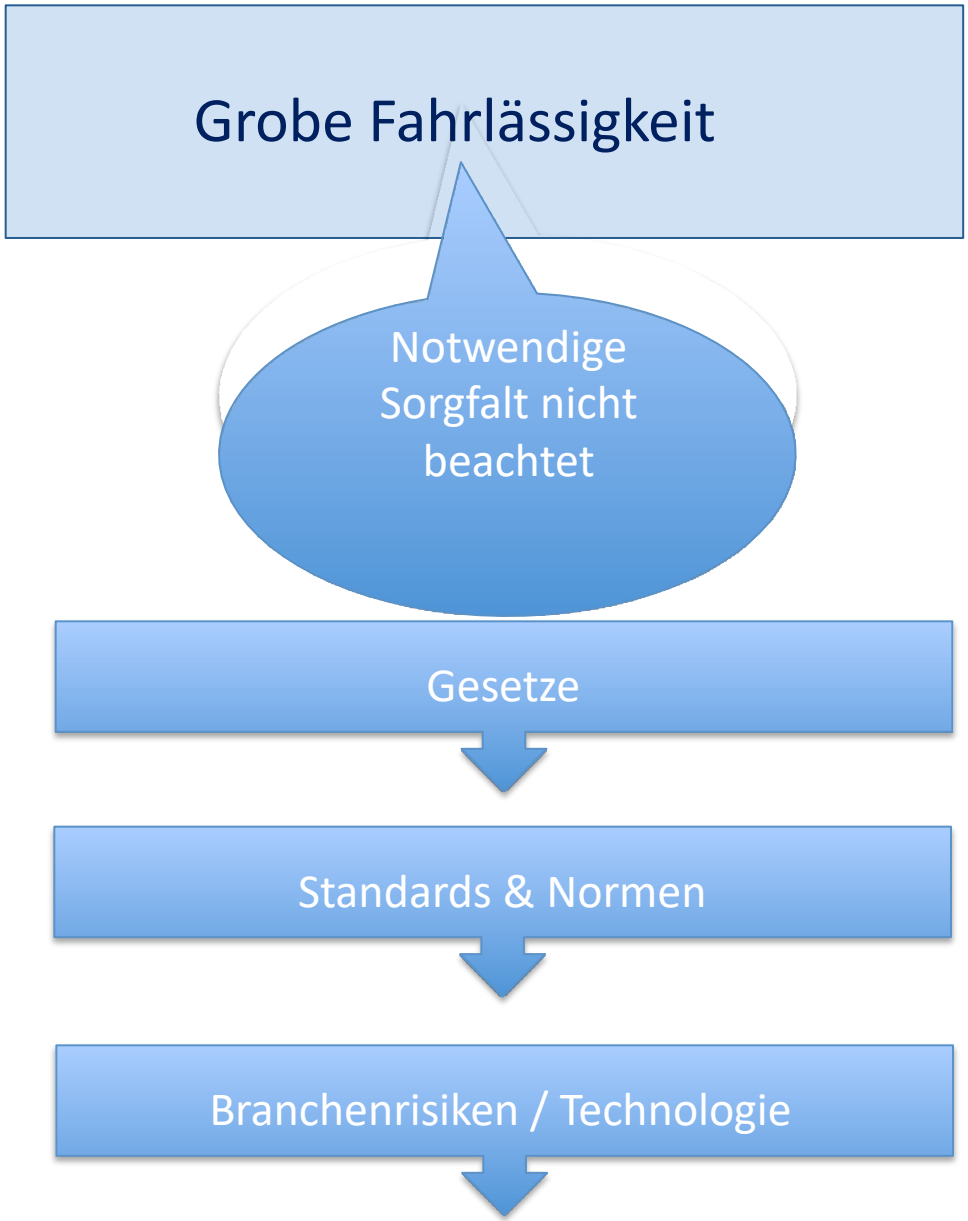
III. Haftung für Verwaltung, Geschäftsführung und Liquidation

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

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Die Sorgfalt richtet sich nach dem Recht, Wissensstand und den Massstäben im Zeitpunkt der fraglichen Handlung oder Unterlassung.


Grobe Fahrlässigkeit
Notwendige Sorgfalt nicht beachtet
Gesetze
Standards & Normen
Branchenrisiken / Technologie

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-meineimfpungen-ch?id=fbbd88e3-0b77-4a1e-8c53-38cd4a92b443

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

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]

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

economiesuisse

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.

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.

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

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.

Teil 3

Grundlagen des neuen Datenschutz- und Datensicherheitsrechts

(DSGVO und nDSG-CH)

Grundprinzipien des neuen europäischen Datenschutzes (DSGVO)

Europäischer Gerichtshof EUGH

Das Safe-Harbor-Urteil des EuGH und die Folgen

https://www.tagesschau.de/wirtschaft/facebook-eugh-103.html

Die ↗Entscheidung 2000/520 der EU-Kommission aus dem Jahr 2000, mit der das durch Safe Harbor hergestellte Datenschutzniveau als angemessen anerkannt wurde, ist ungültig. Die Kommission hätte vor Inkrafttreten von Safe Harbor ausführlich untersuchen müssen, ob das US-amerikanische Recht ein angemessenes Datenschutzniveau tatsächlich zulässt.

- Der massenhafte Zugriff auf personenbezogene Daten ohne irgendeine Differenzierung, Einschränkung oder Ausnahme verstößt gegen den Grundsatz der Verhältnismäßigkeit. (Ziff. 93 des Urteils)

- Feststellung, ob es in den Vereinigten Staaten Vorschriften gibt (Rechtslage und Rechtspraxis), die dazu dienen, etwaige Eingriffe in die Grundrechte der Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, zu begrenzen.

- Wirksamkeit eines gerichtlichen Rechtschutzes gegen derartige Eingriffe.

Neues EU- und CH-Datenschutzrecht

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)

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 Rahmen-beschlusses (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)

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.

(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

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.

Territorialer Geltungsbereich der DSGVO

Marktortprinzip
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)

Anknüpfungspunkt 1

Waren und Dienstleistungen anbieten

(Art. 3 Abs. 2 lit.a DSGVO)

- wenn der **VERANTWORTLICHE** oder der **AUFTRAGSVERARBEITER**
- **WAREN oder DIENSTLEISTUNGEN**
- **offensichtlich in der EU anbieten**

- **Ausrichtung auf EU-Markt muss deutlich erkennbar sein**
- **Aktiv auf das Anbieten von Waren und Dienstleistungen ausgerichtet sein**
- **Unabhängig davon, ob gegen Geld oder kostenlos**
- **Offensichtlich:** reines Bereitstellen eines Internetauftritts oder Publizieren einer E-Mail-Adresse genügt nicht
    - **Spezifische Aktivitäten (Folgefolien)**

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)

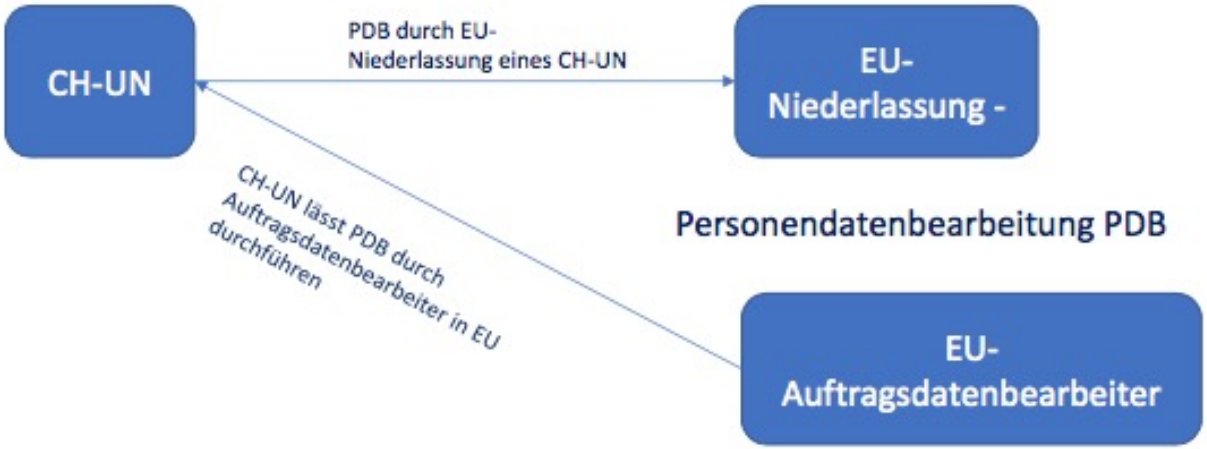
- Kriterium **Zielmarkt**
  AUFENTHALT der von Datenbearbeitung **betroffenen Person in der EU** (§ 3 Abs. 2 DSGVO)
  DER AUFENTHALT des Verantwortlichen ist ausserhalb EU, aber die Datenbearbeitung betrifft Waren oder Dienstleistungen, die für Personen in der EU bestimmt sind oder die Bearbeitung betrifft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

Territoriale Geltung für CH-Unternehmen

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.



PDB: Personendatenverarbeitung

Territoriale Geltung für CH-Unternehmen (4)

Marktortprinzip in Onlinehandel

(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.

Territoriale Geltung für CH-Unternehmen (5)

- **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

Anknüpfungspunkt 2

Überwachen des Verhaltens einer Person in EU

(Art. 3 Abs. 2 lit.b DSGVO)

- wenn der **VERANTWORTLICHE**
  - **die Internetaktivitäten des BETROFFENEN**
  - **nachvollzieht, einschliesslich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten,**
    - **durch die von einem BETROFFENEN ein PROFIL erstellt wird,**
    - **das Grundlage für ihn betreffende Entscheidungen bildet oder**
    - **anhand dessen seine persönliche Verhaltensweisen oder**
    - **Gepflogenheiten analysiert oder vorausgesagt werden sollen.**

Anknüpfungspunkt 2

Überwachen des Verhaltens einer Person in EU (Art. 3 Abs. 2 lit.b DSGVO)

- Wenn Internetaktivitäten von betroffenen Personen nachvollzogen werden
  - Erstellung von Persönlichkeitsprofilen
    - Wenn diese Grundlage für eine Entscheidung der betroffenen Personen bilden
    - Anhand derer die Vorlieben, Verhaltenswiesen oder Gepflogenheiten analysiert oder vorausgesagt werden (ErwGr. 24)
- Wenn Tracking-Cookies eingesetzt werden
- Wenn Social media Plugins eingesetzt werden
- Wenn Browser Fingerprints eingesetzt werden

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 personliche Merkmale wie Leistung, Gesundheit, Aufenthaltsort etc. zu bewerten oder vorherzusage), Social Plugins oder Schaltflächen wie „Like-Button " von Facebook oder „Follower " von Twitter und Instagramm 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 EuGH[7].

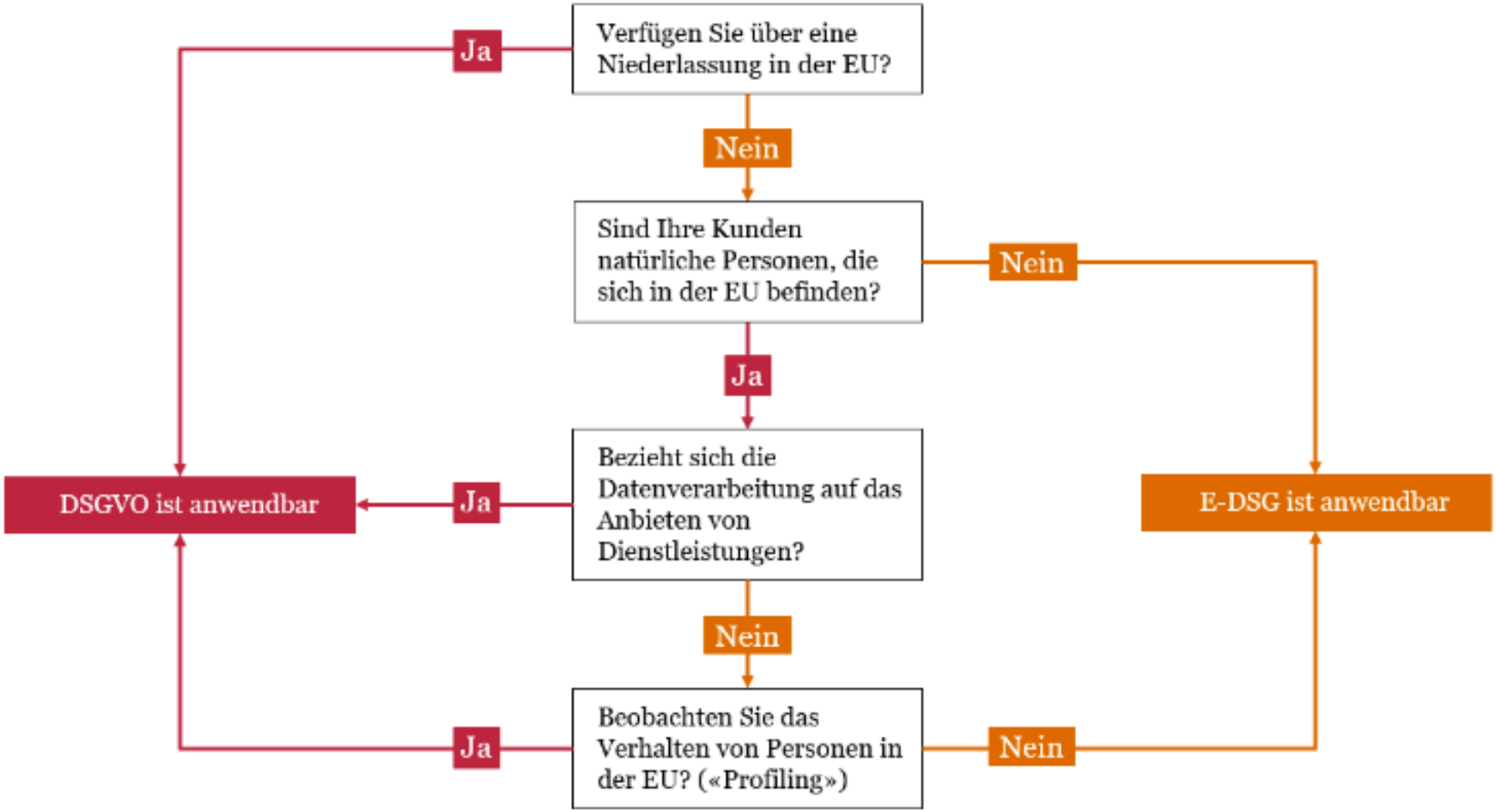
Tracking – Cookies etc.

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.**

Entscheidungsbaum Geltungsbereich



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

Verantwortlicher

Verantwortlicher

Art. 4 § 7 DSGVO / Art. 5 Lit. j nDSG

- **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 / Art. 5 Lit. k und Art. 9 nDSG

- **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)

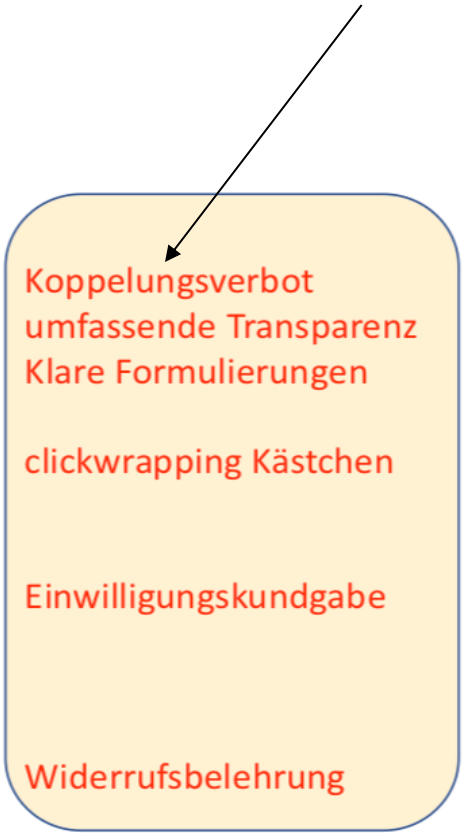
Ausdrückliche Einwilligung

Ausdrückliche Einwilligung

Art. 4 § 11 DSGVO / 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).



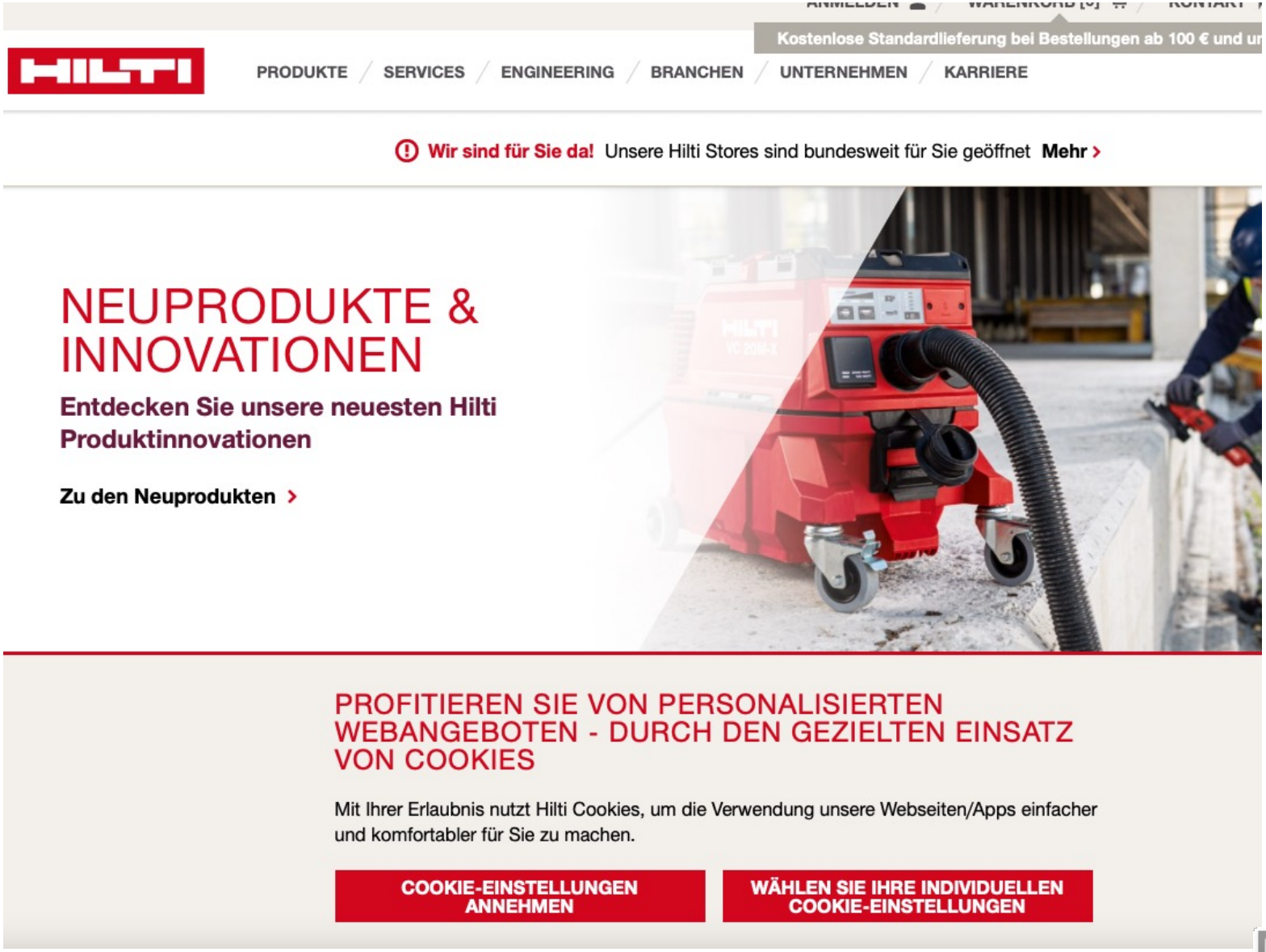
Koppelungsverbot – „Leistung nur bei Einwilligung“

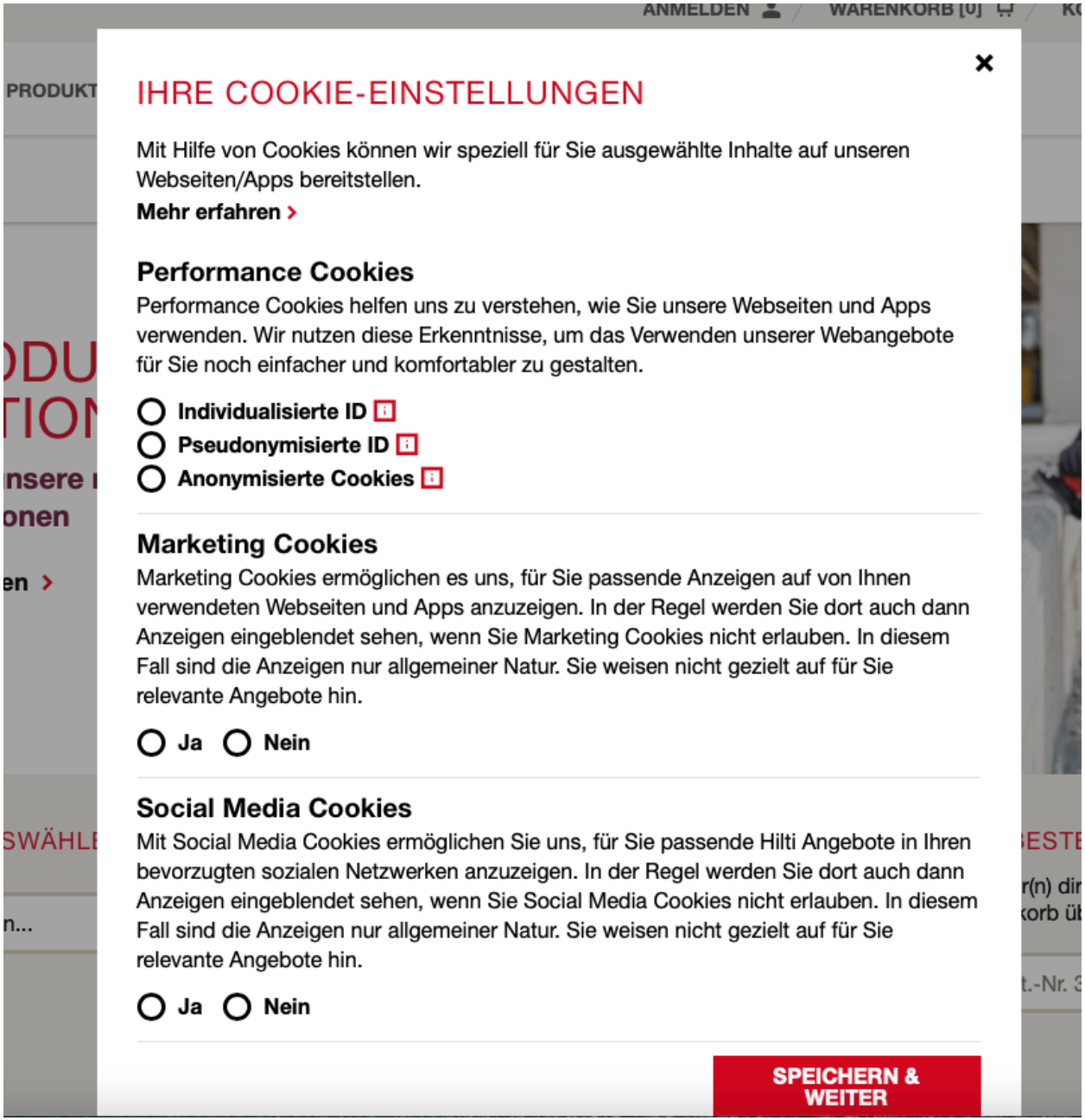
Das Koppelungsverbot ist in Art. 7 Abs. 4 DSGVO geregelt und besagt:

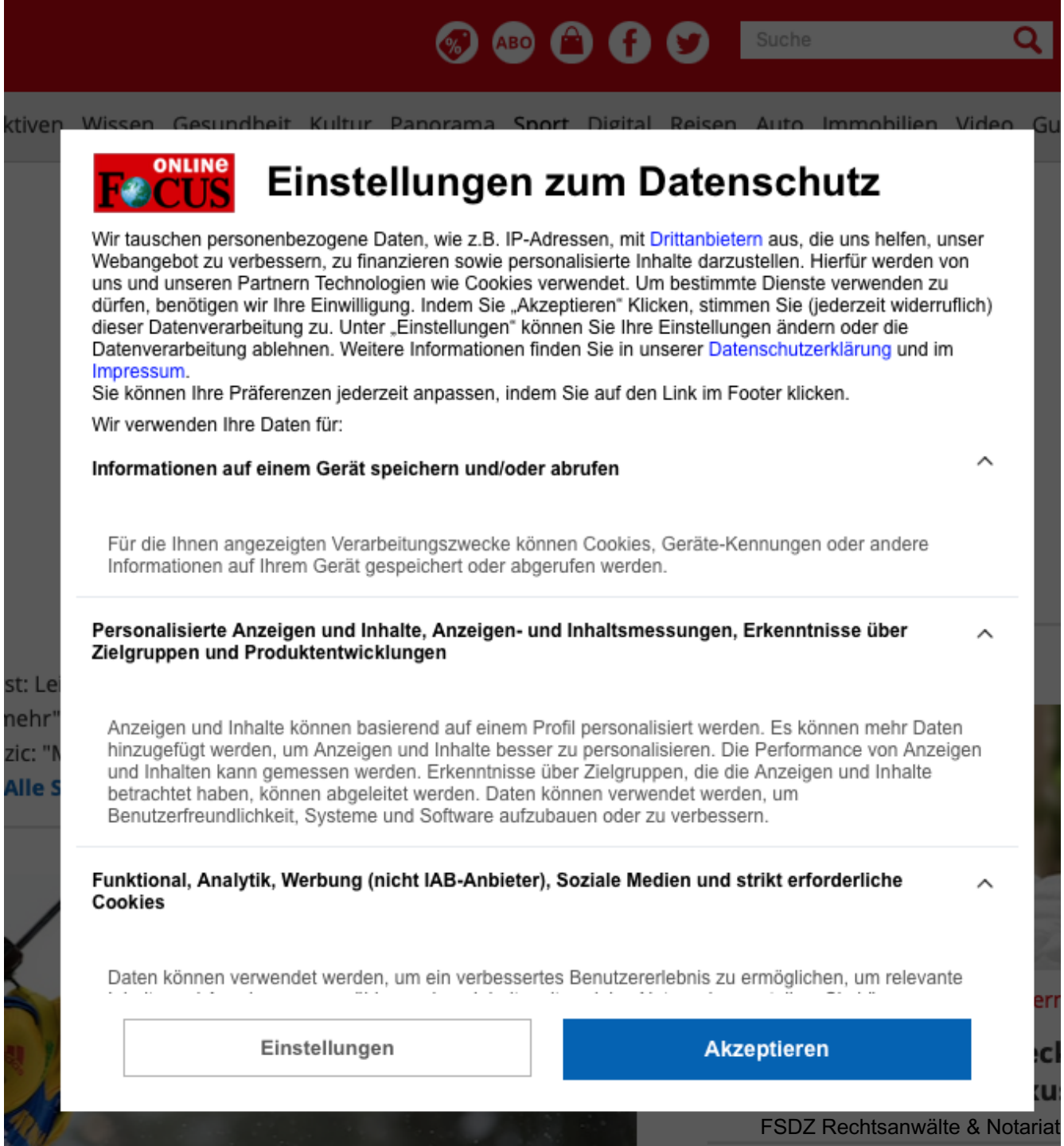
«*Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in grösstmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschliesslich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind*.»

Oberste Gerichtshof in Österreich (OGH) in seinem Urteil zum Koppelungsverbot der DSGVO (Urteil vom 31.08.2018, Az.: 6Ob140/18h). Er stellte fest, dass

«[..] *eine Einwilligung* ***nicht*** *als freiwillig* erteilt *gilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten* ***nicht gesondert eine Einwilligung erteilt werden kann****, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der* ***Erbringung einer Dienstleistung****, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.»*


Kostenlose Standardlieferung bei Bestellungen ab 100 € und ur
HILTI
PRODUKTE / SERVICES / ENGINEERING / BRANCHEN / UNTERNEHMEN / KARRIERE
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]
PRODUKT
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


ABO
Suche
Wissen Gesundheit Kultur Panorama Sport Digital Reisen Auto Immobilien Video
ONLINE FOCUS
Einstellungen zum Datenschutz
Wir tauschen personenbezogene Daten, wie z.B. IP-Adressen, mit Drittanbietern aus, die uns helfen, unser Webangebot zu verbessern, zu finanzieren sowie personalisierte Inhalte darzustellen. Hierfür werden von uns und unseren Partnern Technologien wie Cookies verwendet. Um bestimmte Dienste verwenden zu dürfen, benötigen wir Ihre Einwilligung. Indem Sie „Akzeptieren" Klicken, stimmen Sie (jederzeit widerruflich) dieser Datenverarbeitung zu. Unter „Einstellungen" können Sie Ihre Einstellungen ändern oder die Datenverarbeitung ablehnen. Weitere Informationen finden Sie in unserer Datenschutzerklärung und im Impressum.
Sie können Ihre Präferenzen jederzeit anpassen, indem Sie auf den Link im Footer klicken.
Wir verwenden Ihre Daten für:
Informationen auf einem Gerät speichern und/oder abrufen
Für die Ihnen angezeigten Verarbeitungszwecke können Cookies, Geräte-Kennungen oder andere Informationen auf Ihrem Gerät gespeichert oder abgerufen werden.
Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen
Anzeigen und Inhalte können basierend auf einem Profil personalisiert werden. Es können mehr Daten hinzugefügt werden, um Anzeigen und Inhalte besser zu personalisieren. Die Performance von Anzeigen und Inhalten kann gemessen werden. Erkenntnisse über Zielgruppen, die die Anzeigen und Inhalte betrachtet haben, können abgeleitet werden. Daten können verwendet werden, um Benutzerfreundlichkeit, Systeme und Software aufzubauen oder zu verbessern.
Funktional, Analytik, Werbung (nicht IAB-Anbieter), Soziale Medien und strikt erforderliche Cookies
Daten können verwendet werden, um ein verbessertes Benutzererlebnis zu ermöglichen, um relevante
Einstellungen
Akzeptieren

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

Voreingestellte Einwilligung in Cookies ist unzulässig

Verfasst am 01.10.2019

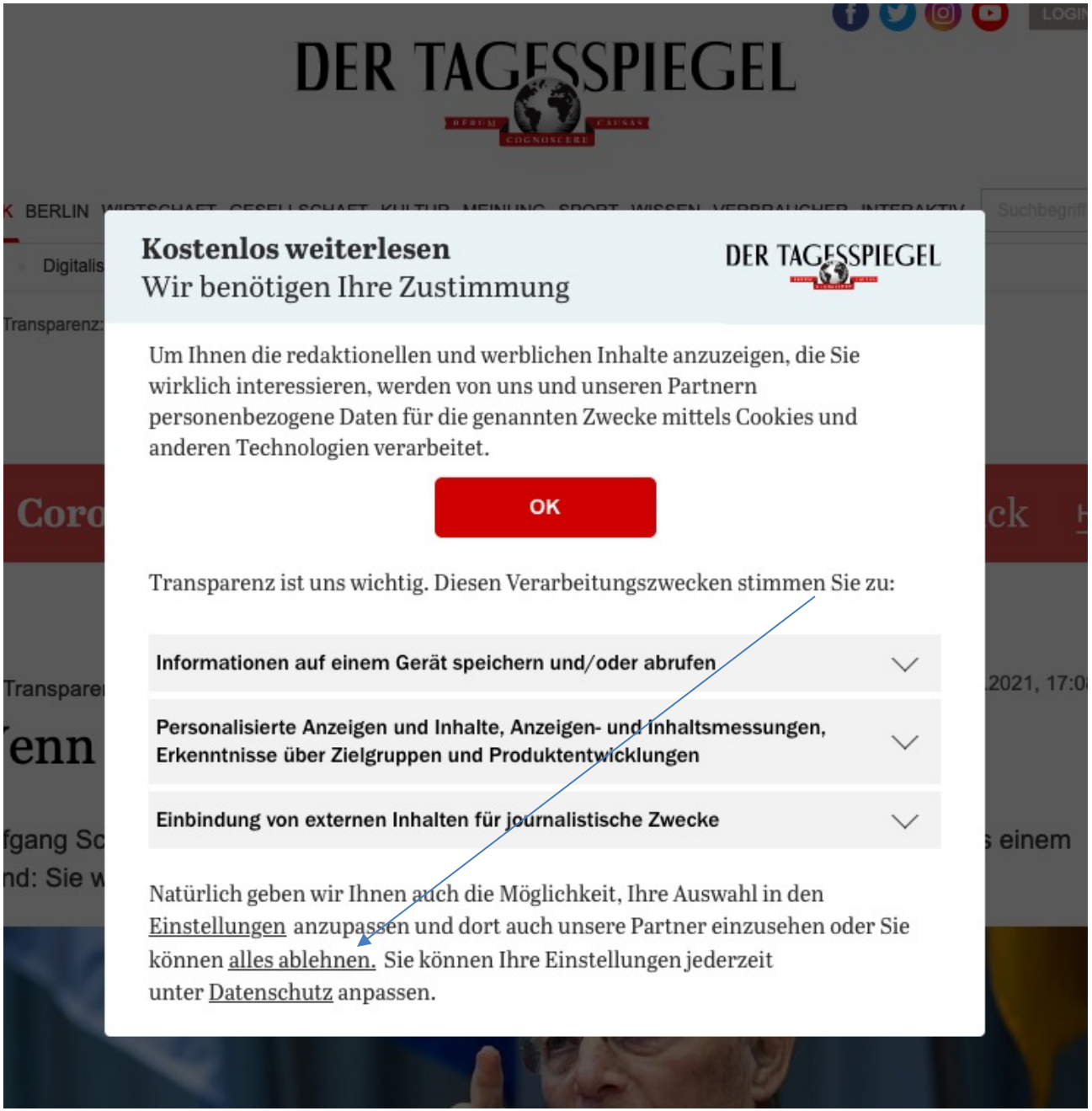
Der EuGH hat mit einem Urteil entschieden, dass die voreingestellte Einwilligung in Cookies unzulässig ist. Die Internetnutzer müssen demzufolge beim Besuch von Webseiten dem Setzen der Cookies aktiv zustimmen.

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


DER TAGESSPIEGEL
Kostenlos weiterlesen
Wir benötigen Ihre Zustimmung
DER TAGESSPIEGEL
Um Ihnen die redaktionellen und werblichen Inhalte anzuzeigen, die Sie wirklich interessieren, werden von uns und unseren Partnern personenbezogene Daten für die genannten Zwecke mittels Cookies und anderen Technologien verarbeitet.
OK
Transparenz ist uns wichtig. Diesen Verarbeitungszwecken stimmen Sie zu:
Informationen auf einem Gerät speichern und/oder abrufen
Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen
Einbindung von externen Inhalten für journalistische Zwecke
Natürlich geben wir Ihnen auch die Möglichkeit, Ihre Auswahl in den Einstellungen anzupassen und dort auch unsere Partner einzusehen oder Sie können alles ablehnen. Sie können Ihre Einstellungen jederzeit unter Datenschutz anpassen.

EuGH-Urteil vom 1.10.2019 – Az. C-673/17 (3)

FSDZ RECHTSANWÄLTE & NOTARIAT AG
ZUGERSTRASSE 76b
CH-6340 BAAR
Tel. ++ 41 41 727 60 80
Fax.++ 41 41 727 60 85
praktikanten@fsdz.ch

SO GEHT MAN AM BESTEN MIT COOKIES UM

7.10.2019

Quelle: https://www.internetworld.de/technik/cookie/so-geht-am-besten-cookies-um-2136695.html

Interne Verfasserin: MLaw Milica Stefanovic

Die User müssen nach dem Entscheid des EuGHs dem Setzen der Cookies aktiv zustimmen. Folgend die Erklärung, was eigentlich hinter den Textinformationen steckt und wie man mit ihnen umgehen sollte.

Das Aufräumen schadet nicht. Die Internet-Nutzer sollten die sogenannten Cookies regelmässig löschen. Das Surfen im Netz ist mit Cookies komfortabler. Die Cookies

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

Carmen De la Cruz
Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin

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

Partnerkanzleien:

Böhni Rechtsanwälte GmbH
Roman Böhni
MLaw Rechtsanwalt,
BSc Wirtschaftsinformatik
Tel: ++41 41 541 79 60
roman.boehni@boehnilaw.ch
www.boehnilaw.ch

de la cruz beranek Rechtsanwälte AG
Carmen De la Cruz

Die beigezogenen Datenverarbeiter

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 beigezogene Service-Provider auslagert, muss einen Auftragsdatenverarbeitungsvertrag (ADVV) 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.

Art. 28 (4) DSGVO / 9 nDSG
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 sind keine qualifizierten eigenhändigen Unterschriften)
- Im Handelsregister eingetragene Personen müssen unterzeichnen (Achtung Kollektivunterschriften beachten)

Meldepflichten

Data Breach Notifications (DSGVO)

Meldung an Datenschutzbehörde

Art. 33 DSGVO

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) [1] Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. [2] Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

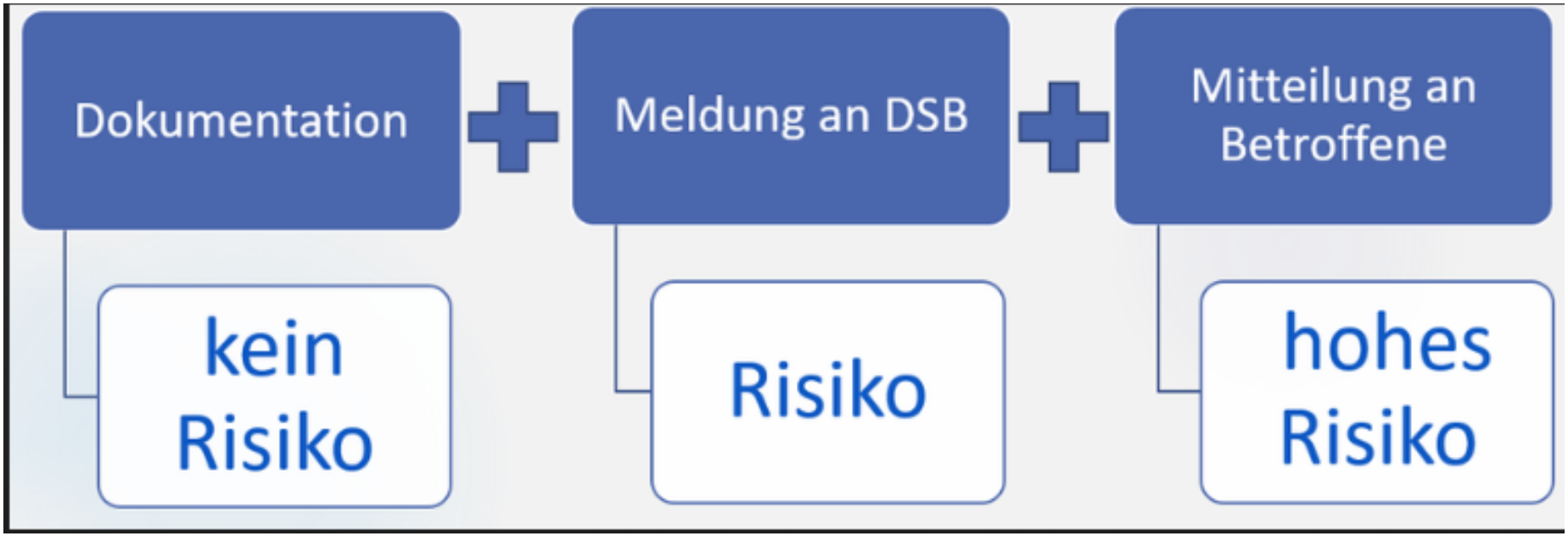
Benachrichtigung an Betroffene

Art. 34 DSGVO

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung

Meldung und Benachrichtigung nach 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

www.eu-datenschutz-vertreter.ch

DSGVO-Pflichten für Unternehmen und Sanktionen

Pflichten der Verantwortlichen

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)

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)

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
    - Muss Register aller Kategorien von Tätigkeiten der UN führen
    - Verantwortliche/Bearbeiter bleibt verantwortlich

Sanktionen 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.

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 |

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

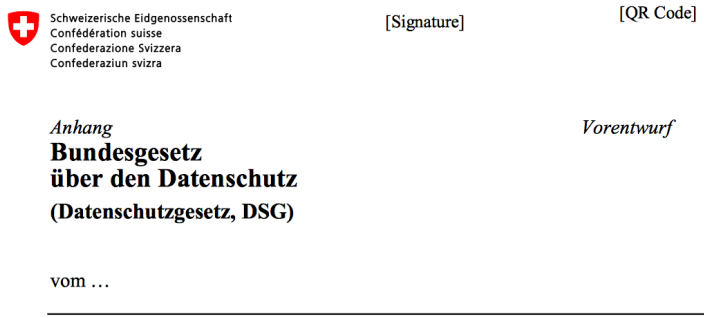
angenommen am 3. Oktober 2017

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

Schweizerisches Bundes-Datenschutzgesetz
(inkl. kantonale DSG)

Grundprinzipien des nDSG

Umsetzung in der CH



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature] [QR Code]

Anhang *Vorentwurf*

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

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. Dauert bis 14.10.2021**
  (https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-84103.html)

- **Inkraftsetzung durch BR in der ohne eine Übergangsfrist von 2 Jahren (im Entwurf noch vorgesehen)**

‹ Laufende Rechtsetzungsprojekte

Stärkung des Datenschutzes

Fragen und Antworten zum Datenschutz

Berichte

Stärkung des Datenschutzes

Es ist vorgesehen, das neue Datenschutzrecht auf den 1. September 2023 in Kraft zu setzen. Der dafür notwendige Entscheid des Bundesrates muss noch erfolgen.

Totalrevision des [B]undesgesetzes über den Datenschutz (DSG)

Konta

Bunde
Daniel
Bunde
CH-30
T +41
F +41
Ko

Schlussabstimmung im Bundesparlament in Bern

25. September 2020

Verordnungsentwurf des BR ist zerzaust worden. Deshalb grösserer Verbesserungsaufwand bei der Verwaltung. Inkrafttreten hinausgeschoben.

Dran bleiben und vorbereiten!!
Sie haben jetzt die „Übergangszeit“ von noch gut 17 Monaten

CH-DSG gilt für Bundesbehörden und Private (Unternehmen)

Kantone erlassen jetzt laufend ihre 26 (!!) neuen kantonalen DSG für ihre kantonalen Verwaltungen und Gemeinden

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

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.

Schweizerisches Zivilgesetzbuch

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

II. Gegen Verletzungen
1. Grundsatz

Art. 28[30]

[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.

Art. 28*a*[31]

2. Klage
a. Im Allgemeinen[32]

1 Der Kläger kann dem Gericht beantragen:

1. eine drohende Verletzung zu verbieten;
2. eine bestehende Verletzung zu beseitigen;
3. die Widerrechtlichkeit einer Verletzung festzustellen, wenn sich diese weiterhin störend auswirkt.

2 Er kann insbesondere verlangen, dass eine Berichtigung oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

3 Vorbehalten bleiben die Klagen auf Schadenersatz und Genugtuung sowie auf Herausgabe eines Gewinns entsprechend den Bestimmungen über die Geschäftsführung ohne Auftrag.

Entwurf nDSG und nVDSG

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature] [QR Code]

Verordnung zum Bundesgesetz über den Datenschutz (VDSG)

vom …

Entwurf in Vernehmlassung

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 2020[1] über den Datenschutz (DSG)

verordnet:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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;

b. Bundesorgane.

Unternehmen sind auch private Personen

Kantone erlassen 26 Kantons-DSG

2 Es ist nicht anwendbar auf:

a. Personendaten, die von einer natürlichen Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden;

b. Personendaten, die von den eidgenössischen Räten und den parlamentarischen Kommissionen im Rahmen ihrer Beratungen bearbeitet werden;

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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 1987[4] über das Internationale Privatrecht. Vorbehalten bleiben zudem die Bestimmungen zum räumlichen Geltungsbereich des Strafgesetzbuchs[5].

Retorsion zu Art. 3 DSGVO

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

2. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Begriffe und Grundsätze

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

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

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)

vom 25. September 2020

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;

Grundsätze der IT-Sicherheit

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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;

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)

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.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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 (ADVV)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature] [QR Code]

Verordnung
zum Bundesgesetz über den Datenschutz
(VDSG)

vom …

Angemessenheit

Art. 1 Grundsätze

[1] Ob die technischen oder organisatorischen Massnahmen zur Gewährleistung der Datensicherheit dem Risiko angemessenen sind, beurteilt sich nach den folgenden Kriterien:

a. Zweck, Art, Umfang und Umstände der Datenbearbeitung;

b. die Eintrittswahrscheinlichkeit einer Verletzung der Datensicherheit und deren potenziellen Auswirkungen für die betroffenen Personen;

c. der Stand der Technik;

d. Implementierungskosten.

[2] Die Massnahmen sind über die gesamte Bearbeitungsdauer hinweg in angemessenen Abständen zu überprüfen.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature] [QR Code]

Schutzziele

Verordnung
zum Bundesgesetz über den Datenschutz
(VDSG)

vom …

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.

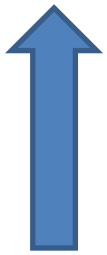
https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

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 konkrete Sicherheitsvorgaben, welche dieser umzusetzen und einzuhalten hat? Wenn ja, welche? Kann er dafür die entsprechenden Vorgaben		

20 Massnahmenvorschläge

https://www.fsdz.ch/file-docs/selbstdeklaration_zum_rahmenvertrag_cloudservices_fmh_-_finale_publikationsversion_2-00_-_14-01-2020.pdf

§ 6

Klassifizierung

[1] Die Informatiksysteme, -anwendungen sowie die Daten und Informationen sind von allen dieser Verordnung unterstehenden Organisationseinheiten nach folgenden Kriterien zu klassifizieren:

a) Verfügbarkeit: Ausfalldauer 3 Tage und mehr (Stufe tief); Ausfalldauer 1 – 3 Tage (Stufe mittel); Ausfalldauer bis ein Tag (Stufe hoch)

b) Vertraulichkeit: Stufe P (public), Stufe N (nicht klassifizierte interne Daten), Stufe V (vertraulich), Stufe G (besonders schützenswert)

c) Integrität: Ausmass einer Beeinträchtigung in der Datennutzung dauert mehrere Jahre (Stufe sehr hoch); maximal bis zu einem Jahr (Stufe hoch); hat einen signifikanten, jedoch nicht über ein Jahr dauernden Einfluss auf das Geschäftsergebnis (Stufe mittel)

d) Nachvollziehbarkeit: keine Nachvollziehbarkeit; anonymisierte Nachvollziehbarkeit; personenbezogene Nachvollziehbarkeit.

e) Beweistauglichkeit und Revisionssicherheit: durch elektronische Signierung und Aufbewahrungsfristen.

Klassifizierung und Schutzziele bestimmen

[1] Die Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank informieren ihre Mitarbeitenden über die Sicherheitsmassnahmen, die sie zu beachten haben.

[2] Sie sorgen für eine periodische Schulung ihrer Mitarbeitenden.

Instruktion des Personals

Mitarbeiter periodisch schulen

Überprüfung

§ 15

[1] Die Inhaber einer Datensammlung und der Betreiber einer zentralen Datenbank überprüfen regelmässig, jedoch mindestens einmal jährlich, die Schutzziele und die Klassifizierung der in ihrem Zuständigkeitsbereich liegenden Informatiksysteme, -anwendungen, Daten und Informationen, die Einhaltung und Angemessenheit der Sicherheitsmassnahmen sowie die Zugangsrechte.

Periodische Prüfung (mindestens 1x jährlich)

- Schutzziele
- Klassifizierung
- Einhaltung der Angemessenheit der Sicherheitsmassnahmen
- Zugangsrechte

Vertretung in der Schweiz

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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.

Informationspflichten

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

Meldepflichten

Data Breach Notifications (nDSG)

Meldung und Benachrichtigung nach nDSG

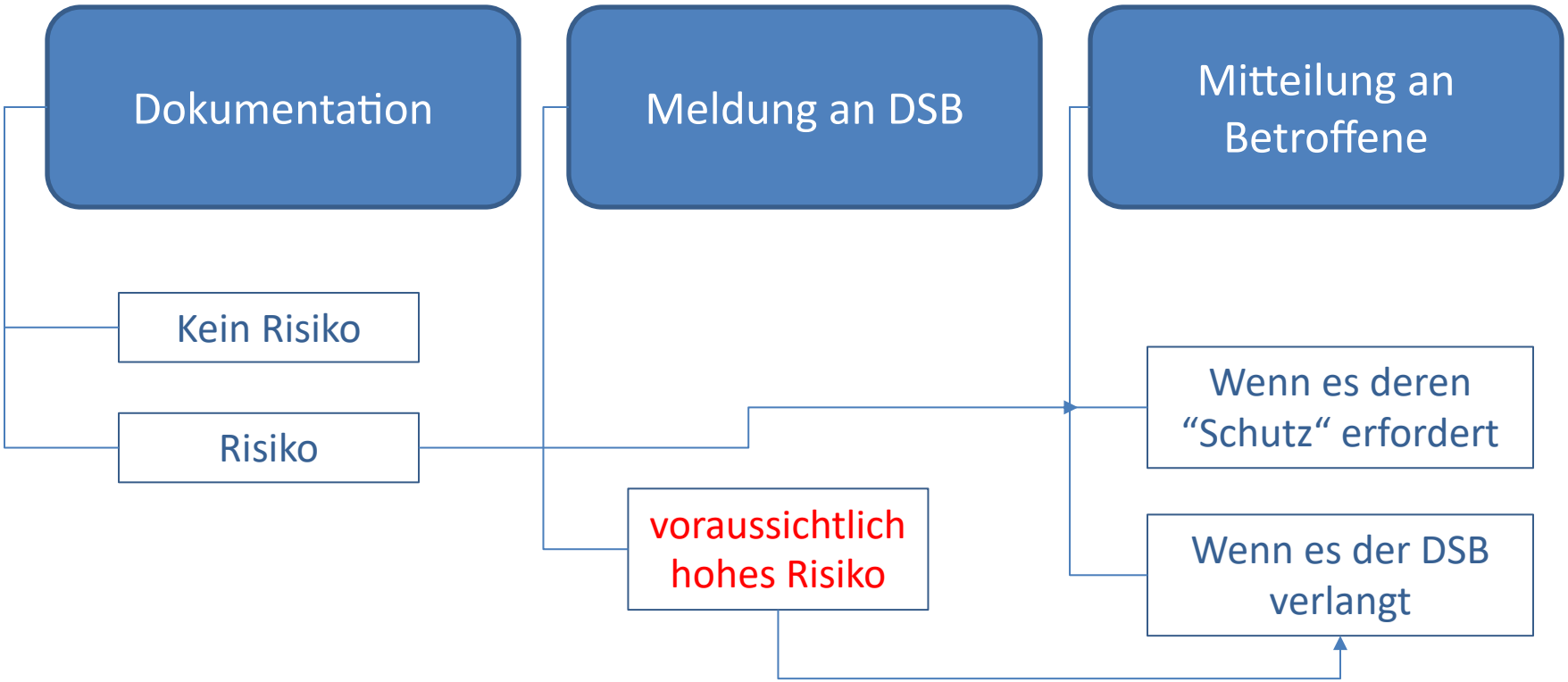
Art. 24 Meldung von Verletzungen der Datensicherheit

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 nDSG

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)

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 EDÖB im Rahmen einer Untersuchung vorsätzlich falsche Auskünfte erteilen oder vorsätzlich die Mitwirkung verweigern.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

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.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgese
über den D nschutz
(Datenschutzg tz, DSG)

vom 25. Septem 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.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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 EDÖB oder einem Entscheid der Rechtsmittelinstanzen, die oder der unter Hinweis auf die Strafdrohung dieses Artikels ergangen ist, vorsätzlich nicht Folge leisten.

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)

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.

Ende Tag 1

Tag 2

Seminar Neues Datenschutzrecht (nCH-DSG und EU-DSGVO)

Tag 1

Seminareinführung
Dr. Bettina Schneider 09.00-09.30

- Big Picture. Einführung zum Seminar
  Warm Up & Kennenlernen

Neues Schweizer DSG und die europäische DSGVO
Lukas Fässler 09.30-12.15

- Neues Schweizer DSG (nCH-DSG)
- Verantwortungsträger im Unternehmen, NPO, Organisationen und öffentlichen Verwaltungen
- Compliance-Vorgaben im Allgemeinen
- Grundlagen des Datenschutzes und der IT-Sicherheit

Mittagspause 12.15-13.15

- Grundprinzipien des neuen Schweizer Datenschutzgesetzes nCH-DSG
- Grundprinzipien der europäischen DSGVO
- Territorialer Geltungsbereich der DSGVO
- Safe Harbor Ade – neue Anforderungen an Data transborder Agreements bis 17.00

Tag 2

Schweizer DSG: Entwicklung eines Datenschutzkonzeptes
Lukas Fässler

- Warm up 09.00-12.15
- Datenschutz:
  Die neuen Instrumente des
- Rechtssicherheit:
  The Roadmap to Compliance
- Datensicherheitskonzept als Bestandteil des Datenschutzes – Prinzipien

Mittagspause 12.15-13.15

- Praxisaufgabe: (Bettina Schneider) 13.15-14.00
  Verarbeitungsverzeichnis
  (Einführung & praktisches Beispiel)
- Praxisaufgabe (Esther Zaugg) 14.15-15.40
  Datenschutzfolgeabschätzung
  (Einführung & Tool)
- Praxisaufgabe: (Lukas Fässler) 16.00-16.45
  Erarbeitung der Data Protection Policy
  (Stufe VR)
- Aufgabenverteilung für Tag 3 bis 17.00

Homework bis zum letzten Kurstag

- Entwurf **Data Protection Policy** fertigstellen und Präsentation vorbereiten
- **Datenschutz-Folge-abschätzung** (DSFA) fertigstellen und Präsentation vorbereiten
- **Verzeichnis von Verarbeitungstätigkeiten** fertigstellen und Präsentation vorbereiten

Tag 3

Schweizer DSG und EU-DSGVO in der Praxis
Lukas Fässler

■ Warm-up	09.00
■ **Data Protection Policies** (Lukas Fässler), in Gruppen, Feedback-Runde	09.10-11.15
■ **Verarbeitungsverzeichnis** (Bettina Schneider), in Gruppen präsentieren, Feedback-Runde	11.15-14.15
Dazwischen Mittagspause	12.15-13.15
■ **Datenschutz-Folgeabschätzung** (Esther Zaugg), in Gruppen präsentieren, Feedback-Runde	14.15-16.15
■ Zusammenfassung, Fragen	bis 16.00

Kurzer Warmup

Die neuen Instrumente des CH-Datenschutzes

Die 7 wichtigsten Umsetzungsaktivitäten für Unternehmen

Personenbezogene Daten (+ Profiling-Daten)	evaluieren
Dokumentationspflichten	erfüllen
Betroffenenrechte – Prozessbeschreibungen	sicherstellen
Organisatorische Massnahmen im Innenverhältnis & im Aussenverhältnis	ergreifen
Technische Massnahmen im Innenverhältnis & im Aussenverhältnis	ergreifen
Neue Verträge mit Datenverarbeitern	ausarbeiten
Internet-Auftritt	überprüfen

MICROSOFT 365 – SERVICES AUS DER MS-CLOUD ANALYSE UND EMPFEHLUNGEN ZUM RRB ZH NR. 2022-0542 - RISIKOGESICHTSPUNKTE

Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 30. März 2022

542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung

1. Ausgangslage

In den letzten Jahren hat sich die Informationstechnologie stark weiterentwickelt. Mit dem Angebot von Cloud-Lösungen entstand ein grundlegend neues, globales Verständnis für den Bezug von Informatikleistungen. Cloud-Lösungen ermöglichen, jederzeit bedarfsgerecht, schnell und flexibel auf standardisierte IT-Angebote zuzugreifen.

Namhafte Softwarehersteller wie Microsoft, Google, Amazon und

Kontroverse Auseinandersetzungen

Diese **Risikobeurteilung** eines lawful-access (z.B. Section 702 des US Foreign Intelligence Surveillance Act (FISA) sowie der Executive Order (EO) 12.333) deckt somit nur einen Teilaspekt der zu klärenden Fragen im Zusammenhang mit der Auslagerung der Bearbeitung von Personendaten und dem Amtsgeheimnis unterliegenden Verwaltungsdaten ab. Sie bezieht sich **ausschliesslich** auf die im Rahmen der IKT-Grundversorgung im Kanton ZH zum Einsatz gelangenden Microsoft-Produkte der M365-Produktefamilie.

Entscheidung der österreichischen Datenschutzbehörde vom 22. April 2022

Rechtsschutzlücken im lokalen Recht dürfen demnach grundsätzlich nicht hingenommen werden und stellen somit keine Frage einer Risikobeurteilung dar.

An alle Interessierten

MICROSOFT 365 – SERVICES AUS DER MS-CLOUD ANALYSE UND EMPFEHLUNGEN ZUM RRB ZH NR. 2022-0542 - RISIKOGESICHTSPUNKTE

Baar, 20. Mai 2022
Von: Rechtsanwalt Lukas Fässler

/Users/martinamurer/Desktop/Microsoft 365 - Cloudservices - Analyse und Empfehlungen zu RRB ZH 2022-0542 - 20-05-2022.docx

01. Ausgangslage

Nach der Veröffentlichung des Beschlusses Nr. 2022-0543 vom 30. März 2022 des Regierungsrates des Kantons Zürich über eine Risikobeurteilung hinsichtlich des Einsatzes von MS365 in der Verwaltung des Kantons ZH sind verschiedene Interpretationen zum Inhalt und der Bedeutung dieses RRB gemacht worden. Einzelne Anfragen gehen soweit, ob es anderen öffentlich-rechtlichen Körperschaften unbesehen weiterer Risikoabklärungen möglich sei, sich auf diesen RRB des Kantons ZH zu stützen und die Auslagerung und den Betrieb gewisser bisher auf internen Servern betriebenen Office-Anwendungen von Microsoft in eine cloud-basierte Umgebung von Microsoft auf diese Risikobeurteilung zuzulassen.

Als Unterlagen haben wir den RRB Nr. 2022-0542, ein Memorandum von VISCHER Rechtsanwälte vom 24.3.2022 (Bischof und Rosenthal) zuhanden des Amtes für Informatik des Kantons Zürich sowie weiterführende und in diesem Dokument verwiesene Entscheidungen mitanalysiert und in unsere Betrachtungen einbezogen.

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

Milica Stefanovic
MLaw Rechtsanwältin[2]
stefanovic@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

Carmen De la Cruz
Rechtsanwältin und Notarin 1,2
Eidg. dipl. Wirtschaftsinformatikerin
Industriestrasse 7
6300 Zug
delacruz@lexcellence.swiss

Partnerkanzleien:

Böhni Rechtsanwälte GmbH
Roman Böhni
MLaw Rechtsanwalt[1,2]
BSc Wirtschaftsinformatik

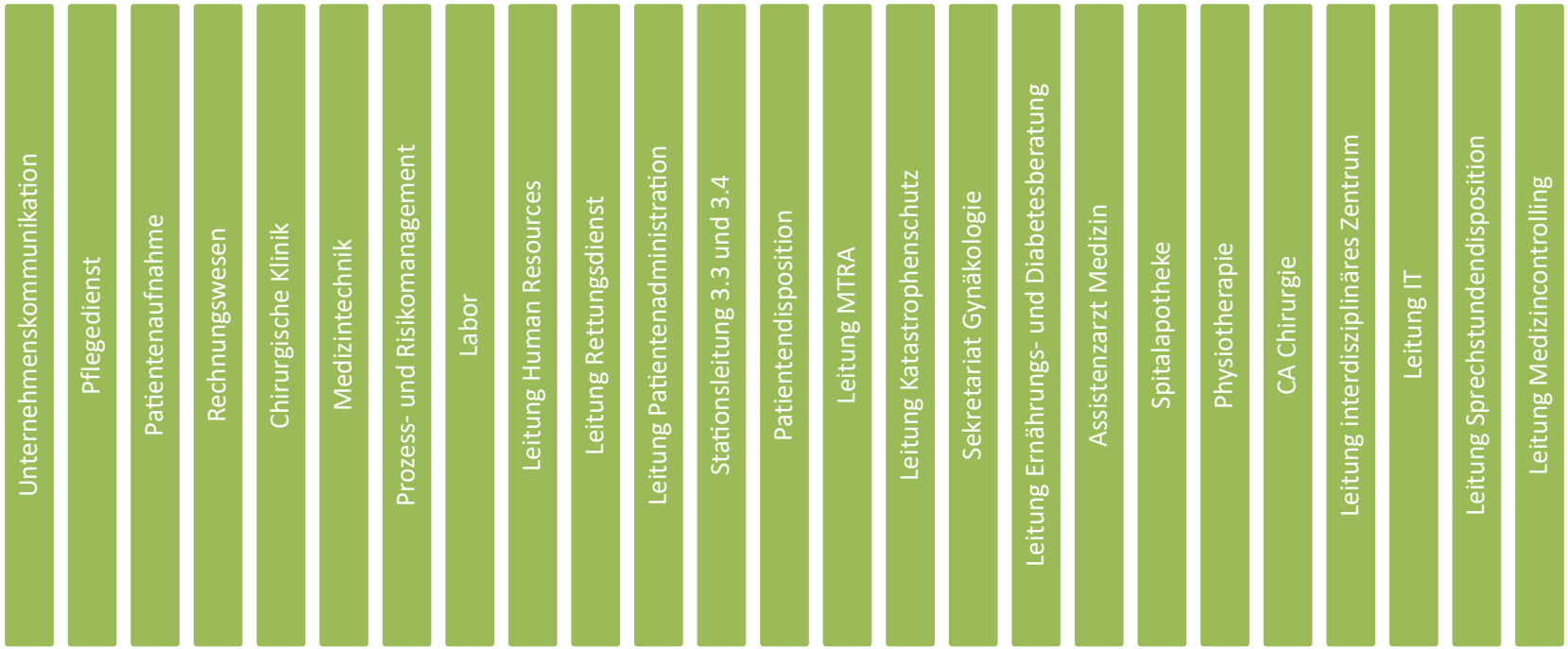
Zugerstrasse 76b
CH-6340 Baar
Tel.: ++41 41 541 79 60
info@boehnilaw.ch
www.boehnilaw.ch

Inventar der Personendaten

Landkarte Personendaten

Unternehmen XY

Unternehmen XY



Spital XY

Patientenaufnahme

Kategorien Personendaten

Personendaten

Besonders schützenswerten Daten

Profilingdaten

Weitere Daten

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) — Muss-Dokument

4. **Vertrag zu Auftragsdatenverarbeitungen** (externe) identifizieren und Verträge (ADDV) mit Service-Providern anpassen. — Muss-Dokument

5. Auslandtransfers identifizieren und offenlegen (DSE)

6. Prozess für Datenschutz-Folgeabschätzung einführen

7. **Datenschutz-Folgeabschätzung** durchführen — Muss-Dokument

8. **Verzeichnis Technische und Organisatorische Massnahmen** (intern und extern) festlegen (allenfalls in neue SLA des ADVV mit Providern einbinden) — Muss-Dokument

Handlungsbedarf unter neuem CH-DSG

9. **Prozesse zur Meldung und Benachrichtigung** von Verletzungen des Datenschutzes und der Datensicherheit einführen

10. 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

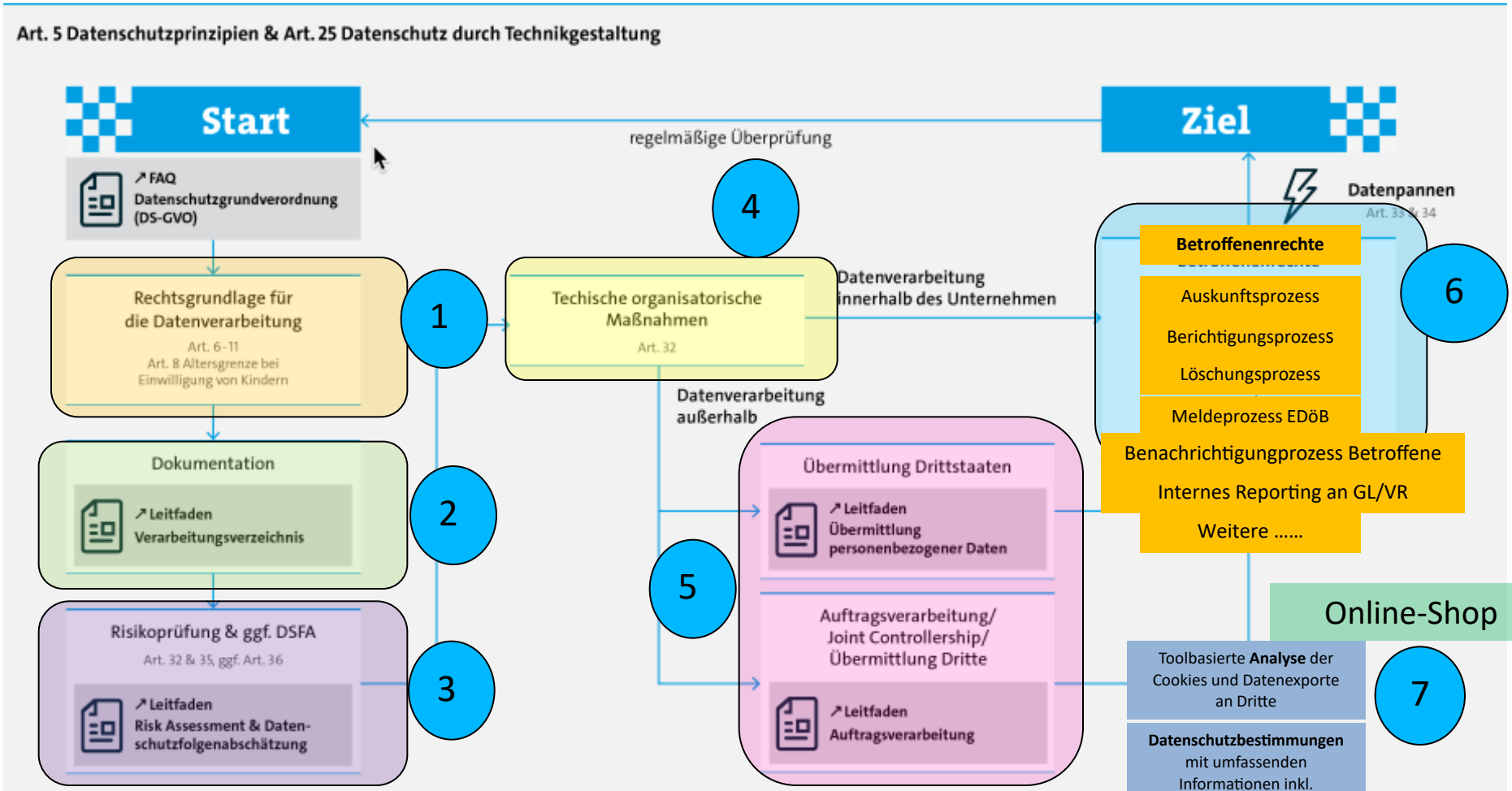
14. Online-Shops **umfassende Informationspflichten** bezüglich Einsatz von Cookies, Profiling-Tools, Targeting-Tools oder Einsatz weiterer Erfassungswerkzeuge prüfen und Datenschutzbestimmungen anpassen. Muss-Anforderung

15. Einwilligungen des Benutzers durch „clickwrapping“ einholen (Modell der diversifizierten Zustimmung vorsehen) Muss-Anforderung

Teil 6:

Rechtssicherheit:
The Roadmap to Compliance

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)

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

Teil 7:

Weiterentwicklungen im Datenschutz der EU

Entschliessung EU-Rat - Verschlüsselung

ZEIT ONLINE

Suche

Politik Gesellschaft Wirtschaft Kultur Wissen **Digital** Campus Arbeit Entdecken Sport ZEITmagazin ze.tt mehr

Überwachung

Der Kampf der EU gegen die Verschlüsselung

Geheimdienste wollen Zugriff auf jede Kommunikation, immer und überall. Die EU-Regierungschefs sind nur zu gern bereit, ihnen bei dem gefährlichen Plan zu helfen.

Von **Kai Biermann**

26. November 2020, 17:56 Uhr / 131 Kommentare /

Entschliessung EU-Rat - Verschlüsselung

Rat der
Europäischen Union

Brüssel, den 24. November 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

https://www.zeit.de/digital/datenschutz/2020-11/verschluesselung.pdf

VERMERK

Absender:	Vorsitz
Empfänger:	Delegationen
Nr. Vordok.:	12863/20
Betr.:	Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung

Die Delegationen erhalten in der Anlage die Entschließung des Rates zur Verschlüsselung.

Achtung: e-Privacy-Verordnung EU

Die neue **ePrivacy-Verordnung (ePVO)** soll die alte **E-Privacy-Richtlinie** (Richtlinie 2002/58/EG) und die Cookie-Richtlinie ersetzen.

Für Werbetreibende und Webseitenbetreiber ist die neue Verordnung von grosser Bedeutung. Auch für Unternehmen in der Schweiz.

Nach der neuen ePVO setzt die Verwendung von Cookies die Zustimmung des Website-Besuchers voraus.

Ohne Einverständnis des Website-Besuchers dürfen nur noch **Cookies verwendet** werden, die **keine Auswirkungen auf seine Privatsphäre** haben (z.B. *Analyse Anzahl Besucher auf Webseite; Besuchszeiten*)

Cookies, die eingesetzt werden, um das **Verhalten des Website-Users** zu **analysieren**, bedürfen der **ausdrücklichen Zustimmung (unambiguous consent)** des Website-Users. Dasselbe gilt, wenn der Betreiber der Website Cookies einsetzt, um den Website-User wiederzuerkennen **(sog. Retargeting)**.

Achtung: e-Privacy-Verordnung EU

Die ePVO wird die Anbieter von **Internet-Browsern** (Internet Explorer, Firefox, Safari, etc.) zwingen, dem Internetnutzer **detailliertere Cookie-Einstellungen** zu ermöglichen.

Jeder Browser wird zukünftig einen "Do-Not-Track-Mechanismus" haben.

Der Browser wird die Cookies von direkt besuchten Websites erkennen und diese je nach Einstellung des Website-Users zulassen.

Gleichzeitig muss der Browser die Cookies von Drittanbietern **(sog. Third PartyCookies)** automatisch erkennen und blockieren.

Achtung: e-Privacy-Verordnung EU

Der lange diskutierte Vorschlag der e-Privacy-Verordnung war im Dezember 2019 fallengelassen worden.

Die Präsidentschaft des Europäischen Rats hat Ende Februar 2020 neue Vorschläge zur Anpassung u.a. des vor allem strittigen Art. 8 des Entwurfs vorgelegt.

Der neue Vorschlag rückt hier vom strikten Einwilligungserfordernis für Bearbeitungen ab, die nicht betriebsnotwendig sind.

Nach dem vorgeschlagenen neuen Art. 8 soll die Verwendung von Cookies und anderen Technologien unter bestimmten Voraussetzungen **auch für berechtigte Interessen** (vgl. Art. 6 Abs. 1 lit. f DSGVO) erlaubt sein.

Ursprünglich war geplant, dass ePrivacy und die DSGVO gleichzeitig in Kraft treten sollen. Von diesem Vorhaben hat man sich längst verabschiedet: Die EU-Mitgliedstaaten können sich seit Jahren **nicht auf eine gemeinsame Linie einigen** und haben zuletzt im November 2020 einen Kompromissvorschlag abgelehnt. Von manchen Ratsmitgliedern wird sogar eine vollkommene Neugestaltung der Verordnung gewünscht. Da in Deutschland auch bei der ePrivacy-Verordnung eine zweijährige Übergangszeit vorgesehen ist, muss man also nicht mit einer plötzlichen Umsetzung eines möglichen, von allen Ländern abgesegneten Entwurfs rechnen. Für 2021 übernimmt nun erst einmal Portugal die Ratspräsidentschaft und tritt damit die Nachfolge von Deutschland und Kroatien an, die 2020 mit ihren Vorschlägen gescheitert waren.

Teil 8:

Bearbeitungsverzeichnis n-DSG

Separate Folienpräsentation
von Dr. Bettina Schneider

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)

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.

Identisch wie Art. 12 nDSG

Teil 9:

Datenschutz-Folgenabschätzung (DSFA) nach nDSG

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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;

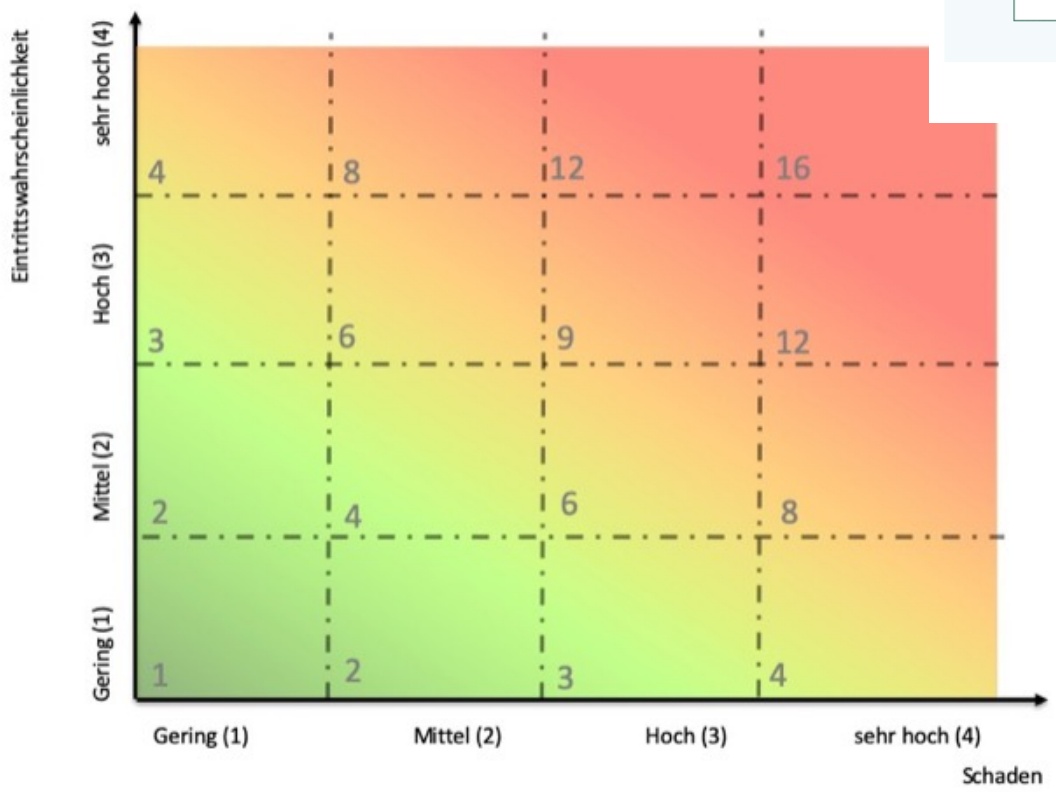
b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden

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

Datenschutz-Folgeabschätzung mit Tool-Vorstellung

Esther Zaugg

Separate Folienpräsentation
von Esther Zaugg

Teil 10:

Praxis-Aufgabe

Lukas Fässler

Erarbeitung einer Data Protection Policy (auf Stufe VR) in Gruppenarbeit

Erarbeiten Sie in den zugewiesenen Arbeitsgruppen eine DPP (**Data Protection Policy**) mit maximal 3 Sätzen, in welchen die strategische Führung (VR) der Unternehmung

- den Stellenwert des Datenschutzes und der Datensicherheit
- die massgeblich anzuwendenden Grundsätze
- die permanente Sicherstellung der Compliance bezüglich Datenschutz und Datensicherheit

in Ihrem Unternehmen festlegt.

Erstellen Sie eine Präsentationsfolie und bestimmen Sie einen Sprecher oder eine Sprecherin für die Gruppe.

Aufgabenverteilung für 18.9.2021

Lukas Fässler
Esther Zaugg
Dr. Bettina Schneider

Ende Tag 2

Tag 3

Tag 3

Schweizer DSG und EU-DSGVO in der Praxis
Lukas Fässler

- Warm-up
- **Data Protection Policies**
  (Lukas Fässler), in Gruppen, Feedback-Runde
- **Verarbeitungsverzeichnis**
  (Bettina Schneider), in Gruppen präsentieren, Feedback-Runde

  Dazwischen Mittagspause
- **Datenschutz-Folgeabschätzung**
  (Esther Zaugg), in Gruppen präsentieren, Feedback-Runde
- Zusammenfassung, Fragen

Kurzer Warmup

Handlungsbedarf unter neuem CH-DSG

1. **Inventar der Personendaten** in Applikationen (interne und externe) und Ablagen mit Speicher- oder Aufbewahrungsort erstellen.

   Startdokument Empfohlen

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 im Gesetz; Empfehlung trotzdem erstellen zwecks Absicherung der Sorgfaltspflichten)

   Muss-Dokument

4. **Vertrag zu Auftragsdatenverarbeitungen** (externe) identifizieren und Verträge (ADDV) mit Service-Providern anpassen.

   Muss-Dokument

5. Auslandtransfers identifizieren und offenlegen (DSE)

6. Prozess für Datenschutz-Folgeabschätzung und kontinuierliche Überprüfung einführen

7. **Datenschutz-Folgeabschätzung** durchführen

   Muss-Dokument

8. **Verzeichnis Technische und Organisatorische Massnahmen** (intern und extern) festlegen (allenfalls in neue SLA des ADVV mit Providern einbinden)

   Muss-Dokument

Handlungsbedarf unter neuem CH-DSG

9. **Prozesse zur Meldung und Benachrichtigung** von Verletzungen des Datenschutzes und der Datensicherheit einführen

Startdokumente Empfohlen

10. Vorgaben und **Prozesse für alle Ersuchen von Betroffenen** erstellen oder anpassen.

Startdokumente Empfohlen

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).

Nachweisdokumente Empfohlen

13. **Angepasste 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

Teil 12:
Data Protection Policy

Rechtsanwalt Lukas Fässler

Präsentationen in Gruppen
Feedback-Runde

Art. 11 Verhaltenskodizes

[1] Berufs-, Branchen- und Wirtschaftsverbände, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind, sowie Bundesorgane können dem EDÖB Verhaltenskodizes vorlegen.

[2] Dieser nimmt zu den Verhaltenskodizes Stellung und veröffentlicht seine Stellungnahmen.

Art. 13 Zertifizierung

[1] Die Hersteller von Datenbearbeitungssystemen oder -programmen sowie die Verantwortlichen und Auftragsbearbeiter können ihre Systeme, Produkte und Dienstleistungen einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.

[2] Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutz-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.

4. Abschnitt: Andere Aufgaben des EDÖB

Art. 56 Register

Der EDÖB führt ein Register der Bearbeitungstätigkeiten der Bundesorgane. Das Register wird veröffentlicht.

Teil 13:
Verzeichnis von Verarbeitungstätigkeiten

Dr. Bettina Schneider

Präsentationen in Gruppen
Feedback-Runde

Teil 14:
Datenschutz-Folgeabschätzung

Esther Zaugg

Präsentationen in Gruppen
Feedback-Runde

Teil 15:
Zusammenfassung und Fragen

Rechtsanwalt Lukas Fässler
Dr. Bettina Schneider
Esther Zaugg

Unterlagen für die Praxis

https://www.bitkom.org

Diverse Checklisten

Datatilsynet

Guide

Software development with Data Protection
Default

The Norwegian Data Protection Authority has devel
help organisations understand and comply with the
protection by design and by default in article 25 of t
Protection Regulation. We have cooperated with se
software developers in public and private sector am

2 Requirements

The checklist is dynamic, not exhaustive, and will be updated regularly. If you have any suggestions or comments, we would like to hear from you.

Requirements for software, products, applications, systems, solutions, or services must:

- fulfil the data-protection principles
- protect the data protection rights of the data subject
- fulfil the company's obligations
- ensure that that settings are by default set to the most privacy-friendly option
- ensure that the end product is robust, secure, and provides enforceability of the data subjects rights

What needs to be done

- Define the processi
  - Will person
  - Identify th
    contracts
    controlle
  - What is
  - What i
  - For hc
    data?
  - Defi
    ach
    pe
    d
    e

5 Testing

The checklist is dynamic, not static, and will be updated regularly. If you have any suggestions or comments, we would like to hear from you.

Test that the requirements for data protection and security that were specified in Requirements have in fact been implemented, and that they are correctly implemented:

- Remember that the data protection regulation also apply to development and testing environments.
- Establish a comprehensive understanding of functionality and information.
- Verify that the requirements and design components have fulfilled the security and data protection requirements. This can, for example, be done by creating standard test scenarios based on functional requirements that can be reused throughout the business.
- Compile a checklist on whether all the components needed for compliance are included. This also includes new components that may not originally have been specified when the requirements were determined. Examples:
  - All settings should be set to the most privacy-friendly option by default.
  - It must be possible to export and import the data subject's data (data portability).
  - Is data being saved in the correct place?
  - Is the data being collected necessary for the purpose of the software?
  - The data subject should be able to give consent (this applies also to children and persons subject to guardians).
  - The data subject must be able to refuse or withdraw consent.
  - Is it possible to terminate a contract/agreement, install, uninstall, activate and deactivate a program, service, technical component, or system?
  - Access control

3 Design

The checklist is dynamic, not exhaustive, and will be updated regularly.
f you have any suggestions or comments, we would like to hear from
ou.

ata oriented design
inimise and limit.** The ar
what is lawful and what
ger required for the p

nples:
Review the Data
Be sure that th
collected. Do
information p
Avoid, limit,
Limit and m
the user int

7 Maintenance (operation)

This checklist is dynamic, not exhaustive, and will be updated regularly. If you have any suggestions or comments, we would like to hear from you.

How to handle incidents and data breaches?

- Implement and operate a plan for incident response management (prepared during the release activity).
- Security incidents must be given high priority.
- Handle incidents and data breaches:
  - **Detect** abnormal activity, traffic, security incidents, and data breaches.
  - **Analyse/Verify** whether abnormal activity, traffic, security incidents, and data breaches are actual security breaches or false positives
  - **Report** security breaches and data breaches according to internal guidelines for incident response handling.
  - **Handle** security incidents and data breaches according to the organisation's continuity plan for restoring the **normal state** of maintenance, service and operation.

t response training covering unexpected scenarios should be done
ically.

ervice and operation

and allocate roles, responsibilities, and authority.
he data subjects' rights and request related to this, such as data access,
tion, deletion, data portability, consent, information, transparency, etc.
usly assess the effectiveness of technical and organisational security
for uncovering vulnerabilities.

urity tests (such as vulnerability analysis and penetration testing,
tinuous automated health checks of software, infrastructure and

Diverse Checklisten (2)

- checklist for content during code testing activity - Norwegische Datenschutzbehörde - 08-12-2017.pdf
- checklist for content during release activity - Norwegische Datenschutzbehörde - 08-12-2017.pdf
- checklist for content in coding activity - Norwegische Datenschutzbehörde - 08-12-2017.pdf
- checklist for setting requirements to the maintenance activity - Norwegische Datenschutzbehörde - 08-12-2017.pdf
- checklist-design for Software Development - Norwegische Datenschutzbehörde - 08-12-2017.pdf
- checklist-requirements for Software-Development - norwegische Datenschutzbehörde - 08-12-2017.pdf
- checklist-training für SW-Entwicklung - Norwegische Datenschutzbehörde - 08-12-2017
- Software development with Data Protection by Design and by Default - Norwegische Datenschutzbehörde - 08-12-2017.pdf

Anforderungen an Cloud-Service-Provider Zertifizierungen von Datenschutz-Konformität nach ISO 27001 und neu nach ISO 27701 und ISO 27018

Unterlagen von Landesdatenschutzbeauftragten (D)

Wie hoch ist das Risiko für die Rechte und Freiheiten der Betroffenen?

Eine Datenschutz-Folgenabschätzung (DSFA) ist eine strukturierte Risikobeurteilung zur Vorab-Bewertung der möglichen Folgen von Datenverarbeitungen. Die DSFA ist dann nötig, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

Unterlagen von Landesdatenschutzbeauftragten (D)

Die Landesbeauftragte für den Datenschutz Niedersachsen

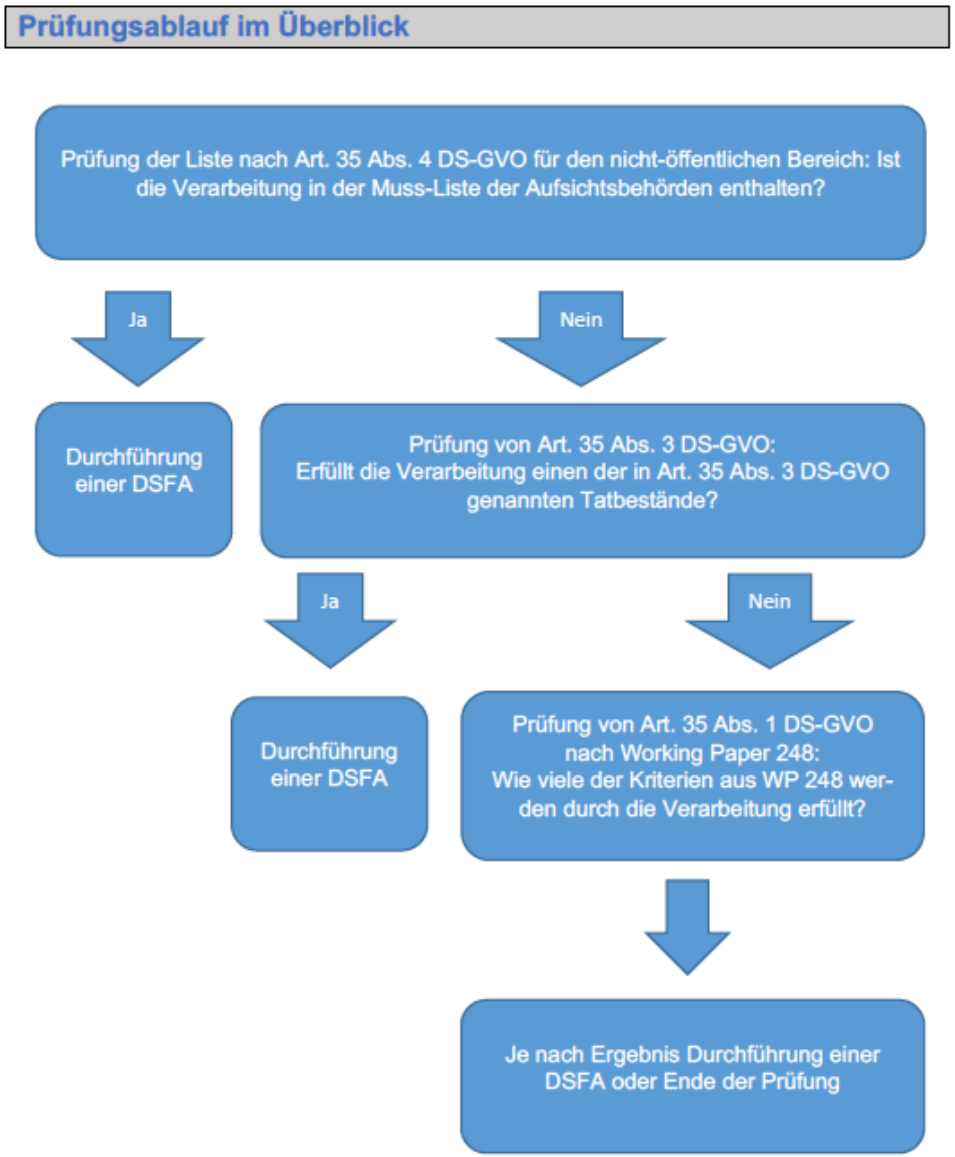
Prüfschema: Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 Datenschutz-Grundverordnung für den nicht-öffentlichen Bereich

Eine Datenschutz-Folgenabschätzung (DSFA) ist eine strukturierte Risikobeurteilung zur Vorab-Bewertung der möglichen Folgen von Datenverarbeitungsvorgängen. Die DSFA ist durchzuführen, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

Mit diesem Prüfschema können Sie für Ihren Verantwortungsbereich prüfen, ob die Durchführung einer DSFA erforderlich ist. Dabei können und sollten (interne oder externe) Datenschutzbeauftragte eingebunden und um Rat gefragt werden. Eine Übermittlung an die Landesbeauftragte für den Datenschutz Niedersachsen ist nicht notwendig.

https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/prufschema_zur_erforderlichkeit_einer_datenschutz_folgenabschatzung/prufschema-muss-ich-eine-datenschutz-folgenabschatzung-durchfuhren-197199.html

Unterlagen von Landesdatenschutzbeauftragten (D)



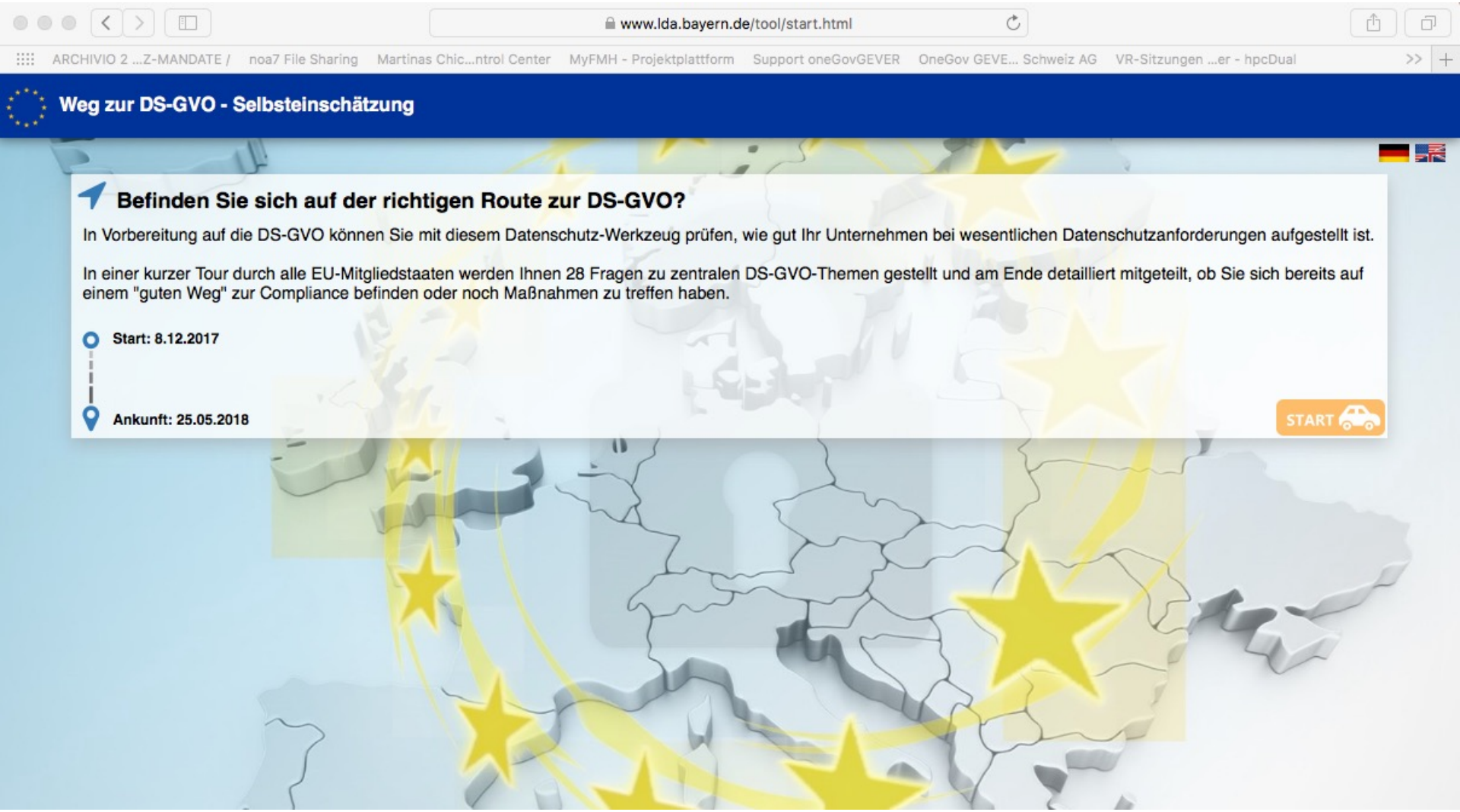
Checkliste

A. Prüfung der Liste nach Art. 35 Abs. 4 DS-GVO		Ja	Nein
A.1	Biometrische Daten zur eindeutigen Identifizierung	☐	☐
A.2	Genetische Daten im Sinne von Artikel 4 Nr. 13 DS-GVO	☐	☐
A.3	Sozial-, Berufs- oder besonderes Amtsgeheimnis	☐	☐
A.4	Daten über den Aufenthalt von natürlichen Personen	☐	☐
A.5	Zusammenführung aus verschiedenen Quellen	☐	☐
A.6	Mobile optisch-elektronische Erfassung in öffentlichen Bereichen	☐	☐
A.7	Bewertung des Verhaltens und anderer persönlicher Aspekte	☐	☐
A.8	Verhalten von Beschäftigten	☐	☐
A.9	Profile über Interessen, Beziehungen oder Persönlichkeit	☐	☐
A.10	Zusammenführung aus verschiedenen Quellen	☐	☐
A.11	Künstliche Intelligenz zur Steuerung der Interaktion oder zur Bewertung persönlicher Aspekte	☐	☐
A.12	Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts oder von Funksignalen	☐	☐
A.13	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit	☐	☐
A.14	Erstellung umfassender Profile über Bewegung und Kaufverhalten	☐	☐
A.15	Anonymisierung von besonderen personenbezogenen Daten zum Zweck der Übermittlung an Dritte	☐	☐
A.16	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO mittels der innovativen Nutzung von Sensoren oder mobilen Anwendungen	☐	☐
A.17	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DS-GVO, um die Leistungsfähigkeit von Personen zu bestimmen	☐	☐

FSDZ Rechtsanwälte & Notariat AG Zug

B. Prüfung von Art. 35 Abs. 3 DS-GVO		Ja	Nein
B.1	Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet	☐	☐
B.2	Umfangreiche Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 Abs. 1 DS-GVO oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DS-GVO	☐	☐
B.3	Systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche	☐	☐

C. Prüfung von Art. 35 Abs. 1 DS-GVO nach Working Paper 248		Ja	Nein
C.1	Betroffene Personen werden bewertet oder eingestuft (Erstellen von Profilen oder Prognosen)	☐	☐
C.2	Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung	☐	☐
C.3	Systematische Überwachung	☐	☐
C.4	Es werden vertrauliche oder höchstpersönliche Daten verarbeitet.	☐	☐
C.5	Datenverarbeitung im großen Umfang	☐	☐
C.6	Datensätze werden abgeglichen oder zusammengeführt	☐	☐
C.7	Daten zu schutzbedürftigen Betroffenen	☐	☐
C.8	Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen	☐	☐
C.9	Die Verarbeitung kann die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern.	☐	☐


www.lda.bayern.de/tool/start.html
ARCHIVIO 2 ...Z-MANDATE /
noa7 File Sharing
Martinas Chic...ntrol Center
MyFMH - Projektplattform
Support oneGovGEVER
OneGov GEVE... Schweiz AG
VR-Sitzungen ...er - hpcDual
Weg zur DS-GVO - Selbsteinschätzung
Befinden Sie sich auf der richtigen Route zur DS-GVO?
In Vorbereitung auf die DS-GVO können Sie mit diesem Datenschutz-Werkzeug prüfen, wie gut Ihr Unternehmen bei wesentlichen Datenschutzanforderungen aufgestellt ist.
In einer kurzer Tour durch alle EU-Mitgliedstaaten werden Ihnen 28 Fragen zu zentralen DS-GVO-Themen gestellt und am Ende detailliert mitgeteilt, ob Sie sich bereits auf einem "guten Weg" zur Compliance befinden oder noch Maßnahmen zu treffen haben.
Start: 8.12.2017
Ankunft: 25.05.2018
START

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

Aktuelles aus unserer Kanzlei.

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
Coperate Governance und Complianc
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 Böhringer
Telefon +41 41 727 60 80
sekretariat@fsdz.ch

e-comtrust international
when trust is on your side
e-comtrust international ag - Zugerstrasse 76b - CH-6340 Baar - +41 41 727 00 70
Start
Dienstleistungen
Über uns
Aktuelles
Referenzen
Kontakt
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
Impressum | erstellt durch Snapdesign

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