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

Profil Kompetenzen Team Aktuell Publikationen Referenzen Kontakt

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

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
Ab 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 Technology Asset Managers Inc. in Amerika

VRP AR Informatik AG	Seit 2019 bis heute
Vizepräsident VR ILZ OW/NW	Seit 2001 bis heute
Vizepräsident VR HIN AG	Seit 2000 bis heute
Präsident Verein SSGI	Seit 2005 bis heute
VRP Viacar AG	Ab Gründung 2010 bis 2012
Dozent Fachhochschule NW in Basel	9 CAS und 2 Seminare
Dozent Universität Basel	Europäisches Marketing- & Wettbewerbsrecht
Dozent Universität Bern/Lausanne	Records Management & Archival Information

Milica Stefanovic

MLaw, Rechtsanwältin

stefanovic@fsdz.ch
+41 41 727 60 80

Profil

seit Dezember 2021
Rechtsanwältin bei FSDZ Rechtsanwälte & Notariat AG

2021
Anwaltspatent des Kantons Luzern

Dezember 2020 - November 2021
Juristische Mitarbeiterin bei FSDZ Rechtsanwälte & Notariat AG

September 2020 - November 2020
Gerichtspraktikum beim Bezirksgericht Hochdorf

August 2019 - Juli 2020
Anwaltspraktikum bei FSDZ Rechtsanwälte & Notariat AG

2019
Master of Law, Universität Luzern

2018
Bachelor of Law, Universität Luzern

Tag 1

Teil 1

Verantwortungsträger im Unternehmen und in öffentlichen Verwaltungen

Busse gegen Meta

Grund der Rekordbusse gegen den Facebook-Mutterkonzern

Aktualisiert am Mittwoch, 24.05.2023, 15:02 Uhr

Die Busse: Wegen schwerwiegender Datenschutzverstösse ist der Facebook-Mutterkonzern von der irischen Aufsichtsbehörde DPC in Dublin zu einer Rekordstrafe in Höhe von 1.2 Milliarden Euro verurteilt worden. Ausserdem dürfen Facebook, Whatsapp und Instagram nach einer Übergangsphase keine Nutzerdaten mehr in die USA übertragen. Facebook hatte jahrelang Daten europäischer Nutzerinnen und Nutzer in die USA transferiert, wo sie von den Geheimdiensten eingesehen werden konnten.

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

Geldbußen für DSGVO-Verstöße

und für Verletzungen anderer Datenschutzgesetze

Nach Land fi... | Suchen

Datum	Bußgeld	Empfänger	Land	Vergehen
10.10.2024	95.533 €	WerepairUK	UK	Durchführung von über 42 Tsd. Werbeanrufen ohne Einwilligung der Empfänger. »Details
10.10.2024	47.766 €	Service Box Group Ltd.	UK	Durchführung von über 5.000 Werbeanrufen ohne Einwilligung der Empfänger. »Details
10.10.2024	50.000 €	SANTANDER CONSUMER	ES	Versand von Werbung trotz Widerspruchs des Empfängers. »Details
08.10.2024	0 €	Unternehmen	FR	Videoüberwachung von Mitarbeitenden. »Details
08.10.2024	0 €	Unternehmen	FR	Unberechtigtes Aufzeichnen und Abhören von Telefongesprächen. »Details
08.10.2024	0 €	Unternehmen	FR	Fehlendes Verzeichnis über Verarbeitungstätigkeiten. »Details
03.10.2024	890.123 €	Police Service of Northern Ireland	UK	Unzureichende Maßnahmen zum Schutz personenbezogener Daten. »Details
02.10.2024	1.999 €	Global Ports's Services	RO	GPS-Überwachung in Firmenwagen und Speicherung der so gesammelten Daten über 6 Monate. »Details
30.09.2024	200.000 €	HM HOSPITALES 1989	ES	Mangelhafte technische und organisatorische Maßnahmen zur Software-Aktualisierung. »Details
27.09.2024	91.000.000 €	Meta Platforms Ireland Ltd.	IE	Speicherung unverschlüsselter Passwörter in internen Datenbanken. »Details

https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/

Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

Zugerstrasse 76b | 6340 Baar | Tel. +41 41 727 60 80 | E-Mail sekretariat

Impressum Datenschutzbestimmungen

Profil Kompetenzen Team Aktuell Publikationen Referenzen Kontakt

Aktuelles aus unserer Kanzlei.

Alle | Intern | Publikationen | Veranstaltungen

IRLAND: Busse von € 345 Mio. gegen TikTok - Verletzung der Informationspflicht und unzureichende TOMs betr. Kinder

Verfasst am 18.09.2023

Die Irischen Datenschutzbehörde hat am 1.9.2023 – nach Konsultation verschiedener weiter involvierten Datenschutzbehörden anderer Länder – und nach Einschaltung und Entscheid der EDSA nach Artikel 65 Abs. 1 lit. a DSGVO – gegenüber TikTok eine Busse von EUR 345 Mio verhängt. Es lagen folgende Verstösse gegen die DSGVO vor:

- Inhalte waren auch für Kinder standardmässig auf "öffentlich" gesetzt
- Mit einer sog. "Familienverknüpfung" konnten Dritte – bspw. Eltern – ihr Konto mit jenem des Kindes verbinden.
- Das Risiko, dass Kinder unter 13 dennoch Zugang zur Plattform erhielten, war nie strukturiert eingeschätzt worden. Eine Datenschutz-Folgenabschätzung lag zwar vor, aber dieses Risiko war ausser Acht gelassen worden.
- TikTok hatte die Informationspflicht verletzt. Dass bei einer «öffentlichen Kontoeinstellung» Dritte, die nicht TikTok-Benutzer waren, Inhalte einsehen konnten, wurde nicht mitgeteilt.

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

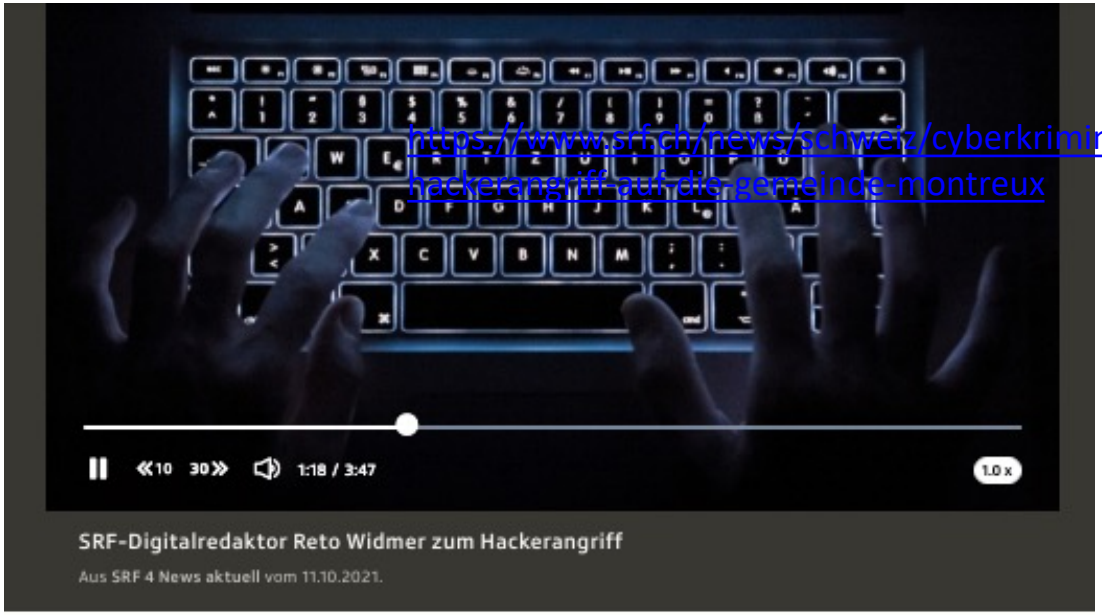
Merken Drucken Teilen

Cyberangriff auf NZZ

Hackerangriff trifft verschiedene Systeme der NZZ und CH Media

Ziel der Attacke seien diverse Dienste der Medien-Unternehmen gewesen. Der Angriff wurde aber frühzeitig erkannt.

Freitag, 24.03.2023, 16:00 Uhr



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

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

Tausende persönliche Daten im Darknet: Die Cyberattacke auf Rolle ist gravierender als von den Behörden kommuniziert

Seit dem Angriff auf die Waadtländer Gemeinde sind sensitive Informationen über Bürger, Mitarbeiter und Unternehmen frei zugänglich. Die Hacker wollten Lösegeld. Der Bund ist eingeschaltet.

Antonio Fumagalli, Lausanne
25.08.2021, 13.49 Uhr

Hören Merken Drucken Teilen

Hackerangriff auf die Firma Xplain: Erste Erkenntnisse aus Datenanalysen zeigen Handlungsbedarf

Bern, 14.06.2023 - Seit Bekanntwerden des Ransomware-Angriffs auf das Unternehmen Xplain laufen in der Bundesverwaltung intensive Abklärungen zu den betroffenen Daten. In den bis heute analysierten Datensätzen finden sich auch operative Daten verschiedener Behörden und Organisationen. Wie diese Daten auf die Infrastruktur der Firma Xplain gelangten, wird nun sorgfältig geklärt.

Am 8. Juni 2023 hat das Nationale Zentrum für Cybersicherheit NCSC kommuniziert, dass sich unter den verschlüsselten und entwendeten Daten der IT-Firma Xplain möglicherweise auch operative Daten aus der Bundesverwaltung befinden. Die

Hackerangriff auf die Firma Concevis: Auch die Bundesverwaltung ist betroffen

Bern, 14.11.2023 - Das Software-Unternehmen Concevis wurde Opfer eines Ransomware-Angriffes, bei dem sämtliche Server der Firma verschlüsselt wurden. Unter den entwendeten Daten befinden sich nach aktuellem Kenntnisstand mutmasslich auch ältere, operative Daten der Bundesverwaltung. Die vertieften Analysen laufen derzeit noch.

Die Firma Concevis, eine Schweizer Anbieterin von Softwarelösungen für öffentliche Verwaltungen (Bund, Kantone, Städte), den Finanzsektor und Unternehmen aus der Industrie und Logistik, ist Opfer eines Ransomware-Angriffs geworden. Die Angreifer entwendeten Daten und verschlüsselten danach sämtliche Server der Firma. Nachdem die Firma der Lösegeldforderung nicht nachgekommen ist, drohen die Angreifer mit der Veröffentlichung der Daten im Darknet.

Hackerangriff legt Login von Schweizer Medienportalen lahm

Nach einem Cyberangriff ist die von etlichen Schweizer Medien genutzte Login-Plattform Onelog nicht verfügbar.

Schweizer Medien-Login nach Cyber-angriff weiter offline

Die Plattform Onelog bleibt ausser Betrieb. Das volle Ausmass des Angriffs ist noch nicht bekannt.

Schweizer Medienplattform Onelog

Cyberangriff auf Stiftsbezirk St. Gallen: Es war Ransomware

Von Philipp Anz, 29. Oktober 2024, 14:59

SECURITY CYBERANGRIFF RANSOMWARE VERWALTUNG KANTON ST. GALLEN

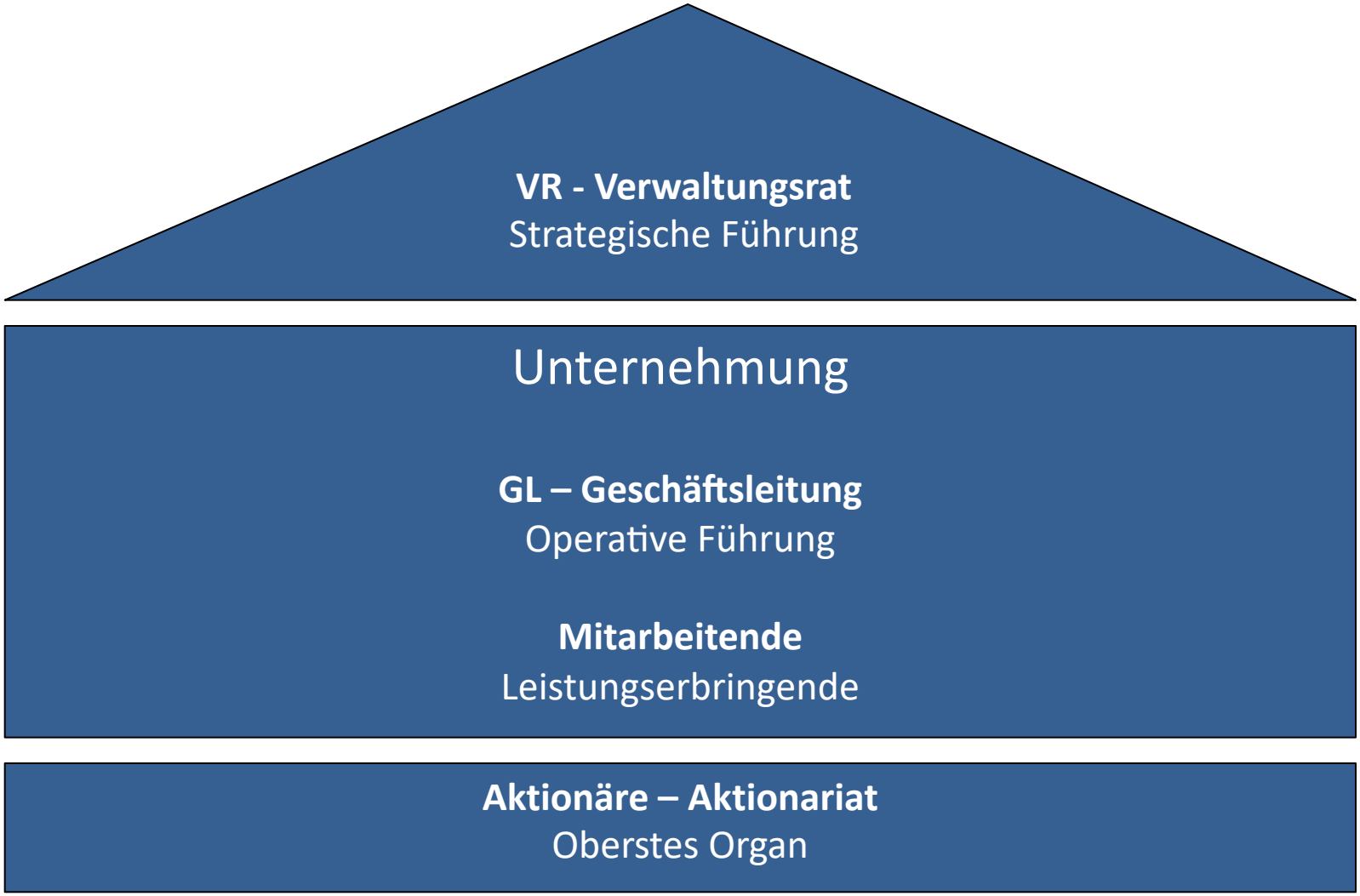
Foto: Bistum St. Gallen

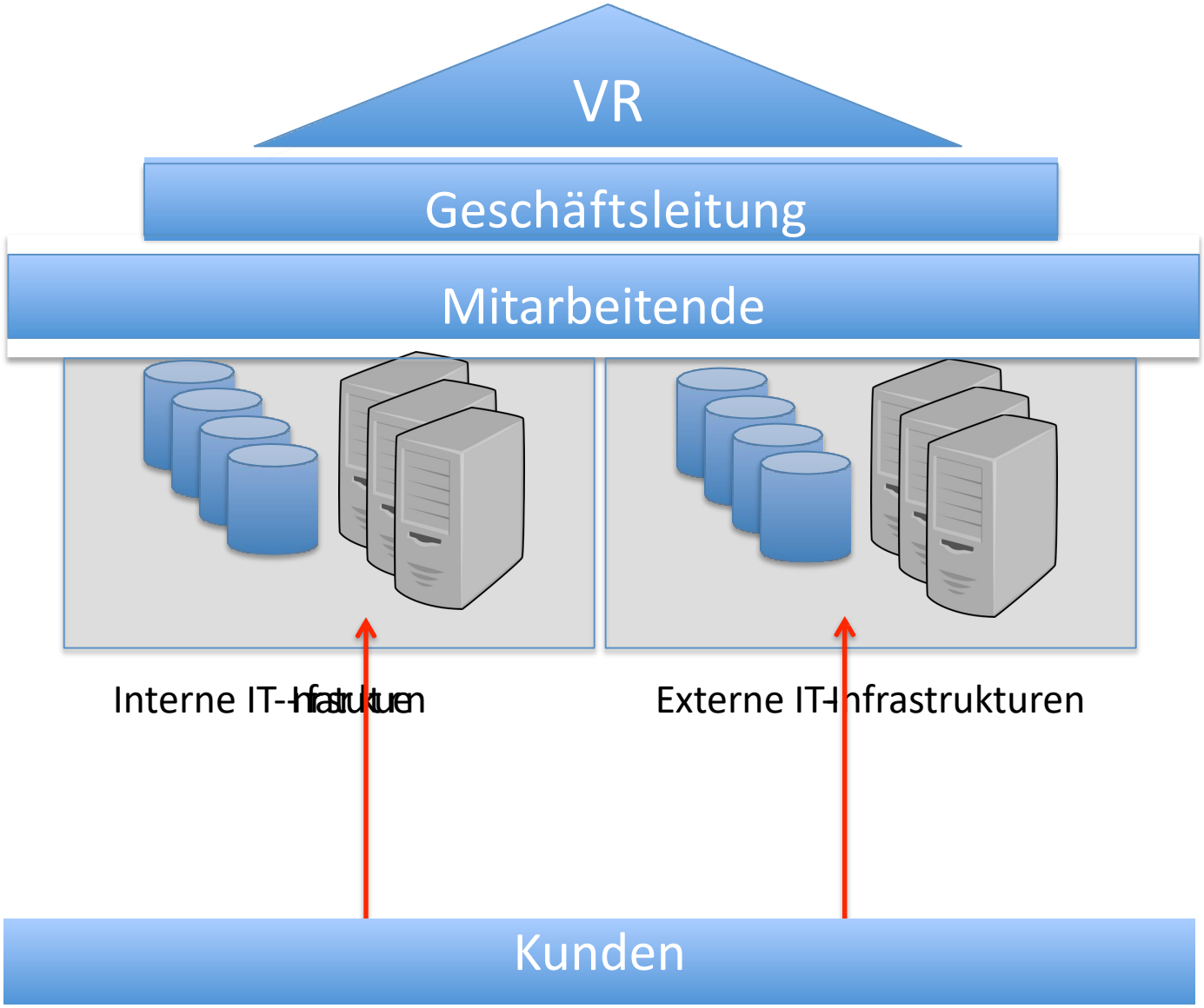
Über den Angriff auf katholische Institutionen in St. Gallen werden neue Details bekannt. Systeme wurden verschlüsselt, eine Lösegeldforderung ist eingegangen.

Am vergangenen Wochenende wurden die kirchlichen Institutionen im Kanton St. Gallen Opfer eines Cyberangriffs. Betroffen sind zahlreiche Einrichtungen des Stiftsbezirks wie unter anderem das Bischöfliches Ordinariat, die Katholische Administration, die Stiftsbibliothek, das Seminar St. Wiborada und die Pensionskasse der Diözese St. Gallen.

Stiftsbezirk St.Gallen

Die Sorgfaltspflichten der Führungskräfte und Mitarbeitenden


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


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

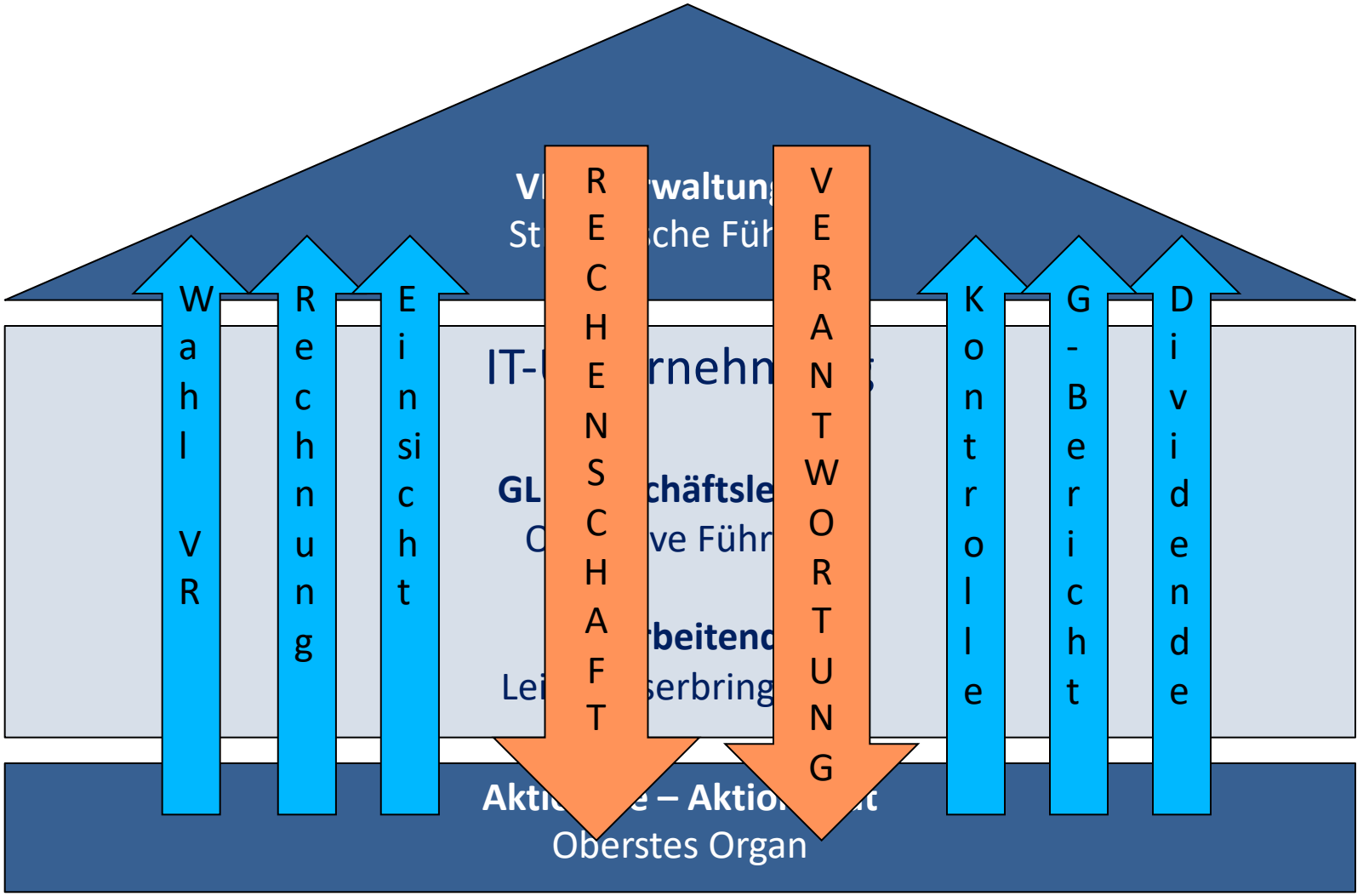
Die gesetzlichen Grundlagen zur Unternehmensführung

Neues Unternehmensrisiko

Compliance zum Datenschutz

Die Generalversammlung der Aktionäre

Aktionäre – Aktionariat
Oberstes Organ


V waltung
St che Füh
IT- rnehm
GL chäftsle
C ve Führ
rbeitend
Lei serbring
Aktio – Aktio t
Oberstes Organ
Wahl VR
Rechnung
Einsicht
RECHENSCHAFT
VERANTWORTUNG
Kontrolle
G-Bericht
Dividende

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

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

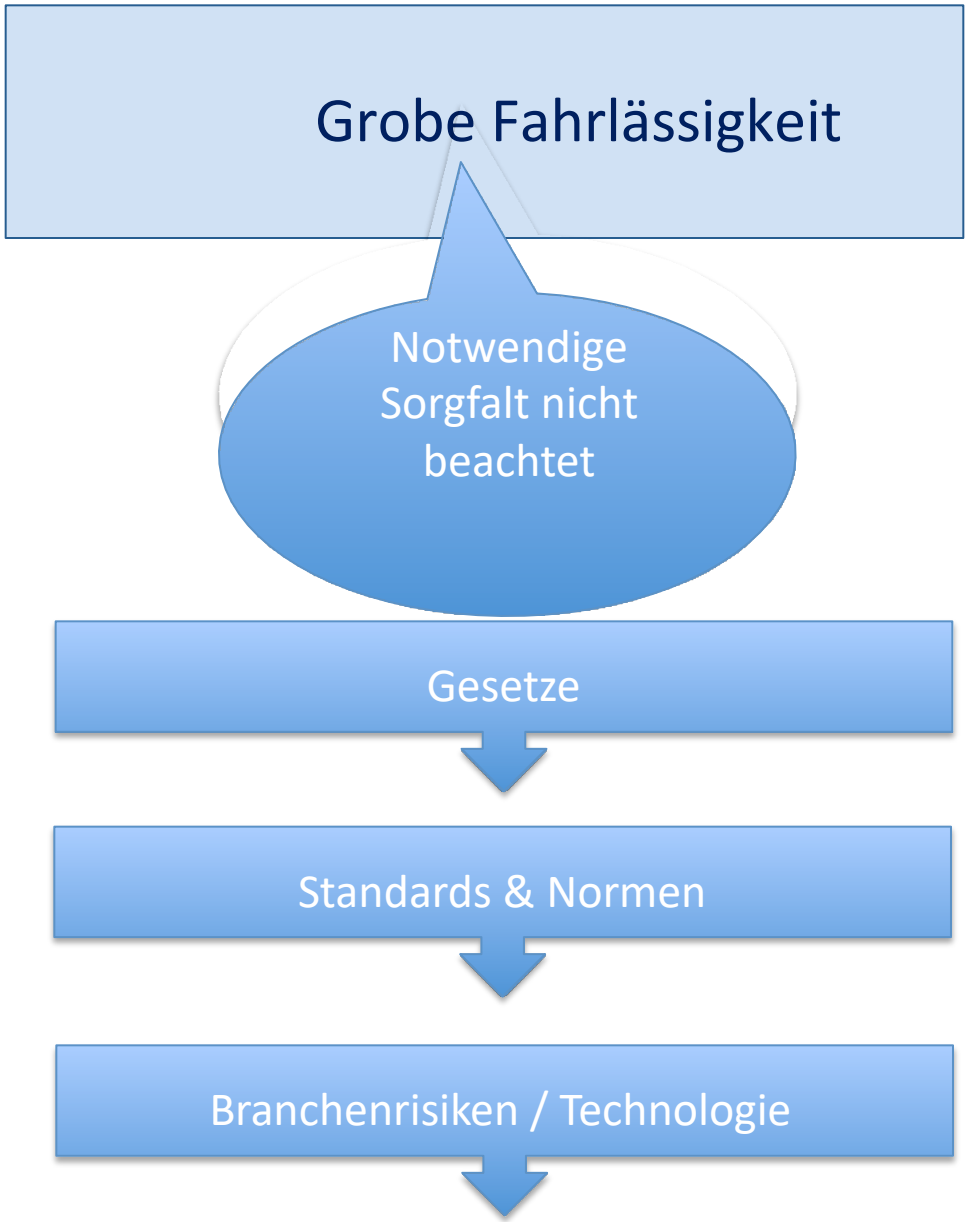
III. Haftung für Verwaltung, Geschäftsführung und Liquidation

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

NEWS

Behörde war zu zurückhaltend

Bundesrat kritisiert BAG im Fall "Meineimpfungen"

Fr 21.04.2023 - 17:02 Uhr
von René Jaun und lha

Laut der Geschäftsprüfungskommission des Nationalrats hätte das Bundesamt für Gesundheit bei der Aufsicht über die Stiftung "Meineimpfungen" rascher und kritischer nachfragen müssen. Ausserdem hätten keine Bundesangestellten im Stiftungsrat sitzen dürfen. Der Bundesrat teilt die Kritik.

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.

Treuepflicht der Arbeitnehmenden

II. Sorgfalts- und Treuepflicht

Art. 321*a*

[1] Der Arbeitnehmer hat die ihm übertragene Arbeit sorgfältig auszuführen und die berechtigten Interessen des Arbeitgebers in guten Treuen zu wahren.

[2] Er hat Maschinen, Arbeitsgeräte, technische Einrichtungen und Anlagen sowie Fahrzeuge des Arbeitgebers fachgerecht zu bedienen und diese sowie Material, die ihm zur Ausführung der Arbeit zur Verfügung gestellt werden, sorgfältig zu behandeln.

[3] Während der Dauer des Arbeitsverhältnisses darf der Arbeitnehmer keine Arbeit gegen Entgelt für einen Dritten leisten, soweit er dadurch seine Treuepflicht verletzt, insbesondere den Arbeitgeber konkurrenziert.

[4] Der Arbeitnehmer darf geheim zu haltende Tatsachen, wie namentlich Fabrikations- und Geschäftsgeheimnisse, von denen er im Dienst des Arbeitgebers Kenntnis erlangt, während des Arbeitsverhältnisses nicht verwerten oder anderen mitteilen; auch nach dessen Beendigung bleibt er zur Verschwiegenheit verpflichtet, soweit es zur Wahrung der berechtigten Interessen des Arbeitgebers erforderlich ist.

Teil 3

Grundlagen des neuen Datenschutz- und Datensicherheitsrechts

(DSGVO und nDSG-CH)

Grundprinzipien des neuen Datenschutz- und Sicherheits-Rechts (DSGVO und nDSG)

Entstehungsgeschichte **Europäisches Datenschutzrecht DSGVO**

- 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.

Europäischer Gerichtshof EUGH

Das Safe-Harbor-Urteil des EuGH und die Folgen

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

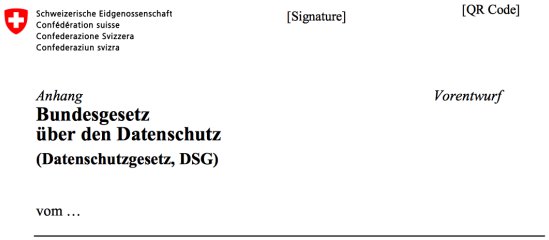
Die ↗Entscheidung 2000/520 der EU-Kommission aus dem Jahr 2000, mit der das durch Safe Harbor hergestellte Datenschutzniveau als angemessen anerkannt wurde, ist ungültig. Die Kommission hätte vor Inkrafttreten von Safe Harbor ausführlich untersuchen müssen, ob das US-amerikanische Recht ein angemessenes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

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. Wurde in der Zwischenzeit überarbeitet und publiziert.**
- **Der Bundesrat hat Datenschutzgesetz, Verordnung zum Datenschutzgesetz und eine Zertifizierungs-Verordnung am 31.8.2022 in Kraft gesetzt auf den 1.9.2023**
- **https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-90134.html**

Geltungsbereich Bund – Kantone - Private

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. Marz 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.

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)

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.

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)

Bearbeitung von Personendaten

vom 25. September 2020

Die Bundesversammlung der Schweizerischen Eidgenossenschaft,
gestützt auf die Artikel 95 Absatz 1, 97 Absatz 1, 122 Absatz 1 und 173 Absatz 2 der Bundesverfassung[1],
nach Einsicht in die Botschaft des Bundesrates vom 15. September 2017[2],
beschliesst:

1. Kapitel: Zweck und Geltungsbereich sowie Aufsichtsbehörde des Bundes

Art. 1 Zweck

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden.

Grundsätze

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

«$$e-seal» «$$QrCode»

Verordnung über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

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 Datenschutzgesetzes vom 25. September 2020[1] (DSG),

verordnet:

1. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Datensicherheit

Art. 1 Grundsätze

[1] Zur Gewährleistung einer angemessenen Datensicherheit müssen der Verantwortliche und der Auftragsbearbeiter den Schutzbedarf der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen.

[2] Der Schutzbedarf der Personendaten wird nach den folgenden Kriterien beurteilt:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

«$$e-seal» «$$QrCode»

Verordnung über Datenschutzzertifizierungen
(VDSZ)

vom 31. August 2022

Der Schweizerische Bundesrat,

gestützt auf Artikel 13 Absatz 2 des Datenschutzgesetzes vom 25. September 2020[1] (DSG),

verordnet:

1. Abschnitt: Zertifizierungsstellen

Art. 1 Anforderungen

[1] Stellen, die Datenschutzzertifizierungen nach Artikel 13 DSG durchführen (Zertifizierungsstellen), müssen akkreditiert sein. Die Akkreditierung richtet sich nach der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1996[2] (AkkBV), soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält.

Teil 4:
Voraussetzungen und Grundprinzipien

Voraussetzungen zur Anwendung des DSG

1. Bearbeitung von Personendaten natürlicher Personen

2. Nur erlaubt, wenn Rechtfertigungsgrund vorhanden

3. Verantwortliche & Auftragsbearbeiter als neue Rollen

4. Schutzbedarf bestimmen (Datenschutzfolgeabschätzung DSFA)

5. Risikobezogene technische & organisatorische Massnahmen (TOM‘s) festlegen

Personendaten

Kategorien

2. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

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

1

b. *betroffene Person:* natürliche Person, über die Personendaten bearbeitet werden;

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;

2

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;

e. *Bekanntgeben:* das Übermitteln oder Zugänglichmachen von Personendaten;

2. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

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;

3a

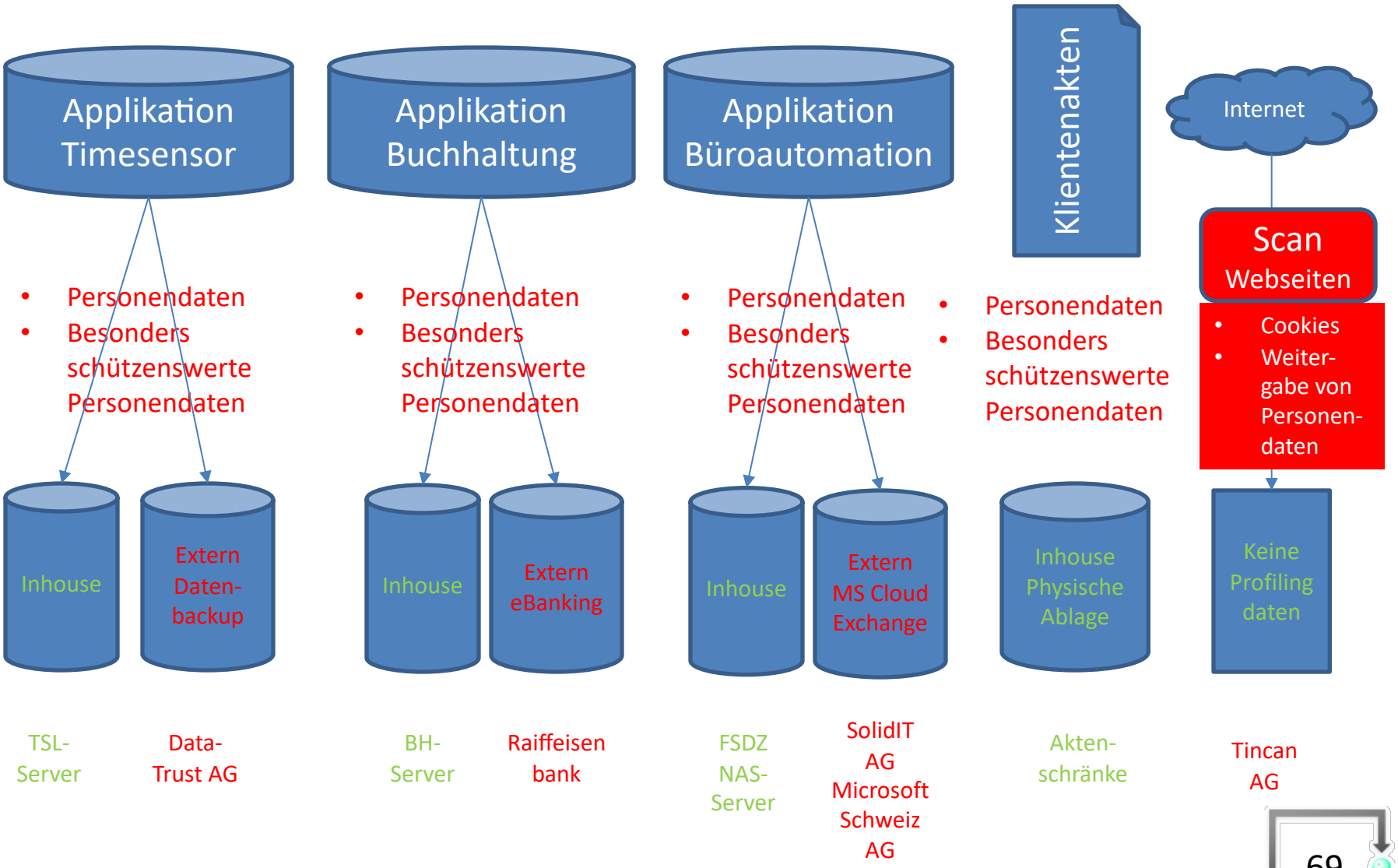
g. *Profiling mit hohem Risiko:* Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

3b

Initialfrage

Bearbeiten wir Personendaten natürlicher Personen?

Inventar der Personendaten



Rechtfertigungsgrund für die Personendatenbearbeitung

Worauf stützen wir unsere Personendatenbearbeitung?

Zulässigkeit der Bearbeitung von Personendaten

1. Gesetzliche Grundlage
2. Ausdrückliche Einwilligung
3. Überwiegendes öffentliches Interesse
4. Überwiegendes privates Interesse

Überwiegendes privates Interesse

Art. 31 Rechtfertigungsgründe

[1] Eine Persönlichkeitsverletzung ist widerrechtlich, wenn sie nicht durch Einwilligung der betroffenen Person, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

[2] Ein überwiegendes Interesse des Verantwortlichen fällt insbesondere in folgenden Fällen in Betracht:

a. Der Verantwortliche bearbeitet die Personendaten über die Vertragspartnerin oder den Vertragspartner in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags.

b. Der Verantwortliche steht mit einer anderen Person in wirtschaftlichem Wettbewerb oder wird in wirtschaftlichen Wettbewerb treten und bearbeitet zu diesem Zweck Personendaten, die Dritten nicht bekanntgegeben werden; nicht als Dritte im Rahmen dieser Bestimmung gelten Unternehmen, die zum selben Konzern gehören wie der Verantwortliche.

c. Der Verantwortliche bearbeitet Personendaten zur Prüfung der Kreditwürdigkeit der betroffenen Person, wobei die folgenden Voraussetzungen erfüllt sind:

1. Es handelt sich weder um besonders schützenswerte Personendaten noch um ein Profiling mit hohem Risiko.
2. Die Daten werden Dritten nur bekanntgegeben, wenn diese die Daten für den Abschluss oder die Abwicklung eines Vertrags mit der betroffenen Person benötigen.
3. Die Daten sind nicht älter als zehn Jahre.
4. Die betroffene Person ist volljährig.

TH

infolaw-th-request@listserv.dfn.de <infolaw-th-request@listserv.dfn.de>

Im Auftrag von Thomas Hoeren <infolaw-th@listserv.dfn.de>

An: infolaw-th@listserv.dfn.de

Donnerstag, 19. September 2024 um 07:09

EuGH Urteil vom 12.09.2024 - C-17/22, C-18/22

Der EuGH hat in dem Vorabentscheidungsersuchen des AG München, eingereicht beim EuGH am 07.01.2022, am 12.09.2024 auf die Vorlagefragen des Gerichts das Spannungsfeld der DS-GVO zum Handelsrecht erläutert, die Grundsätze des europäischen Datenschutzrechts klargestellt und zudem die Rechtssache zurück an das AG München verwiesen.

Demnach kann eine Verarbeitung personenbezogener Daten nach Art 6 I DS-GVO nur dann auf ein berechtigtes Interesse gestützt werden, wenn sie zur Verwirklichung des berechtigten Interesses absolut notwendig ist und unter Würdigung aller relevanten Umstände die Interessen oder Grundrechte und Grundfreiheiten der betreffenden Gesellschafter gegenüber diesem berechtigten Interesse nicht überwiegen. Eine Rechtfertigung hierzu besteht, wenn die Verarbeitung zur Erfüllung von rechtlichen Verpflichtungen erforderlich ist.

Das Urteil schränkt das bisher angenommene Auskunftsrecht von Gesellschaftern einer Publikums-Kommanditgesellschaft hinsichtlich der Kontaktdaten mittelbar über Treuhandgesellschaften beteiligter Mitgesellschafter erheblich ein. Es stellt klar, dass die Weitergabe solcher Daten datenschutzrechtlich nur unter engen Voraussetzungen zulässig ist und insbesondere dann ausscheidet, wenn der zugrundeliegende Beteiligungs- oder Treuhandvertrag dies nicht ausdrücklich zulässt.

Volltext: https://curia.europa.eu/juris/document/document.jsf?text=&docid=290003&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=3379361

PUBLIKATION

Werbung & Datenschutz – EuGH klärt berechtigtes wirtschaftliches Interesse bei Datenkäufen

Quelle: EuGH, 04.10.2024 - C-621/22 - dejure.org (Entscheid im Volltext)

Interner Verfasser: Elena Martin

30. Oktober 2024

Das Urteil des Europäischen Gerichtshofs (EuGH) in der Rechtssache C-621/22 vom 4. Oktober 2024 befasst sich mit der Frage, ob ein berechtigtes Interesse die Weitergabe von Mitgliederdaten durch einen Sportverband an Sponsoren zu Werbezwecken rechtfertigen kann.

Hier sind die wichtigsten Punkte einfach erklärt:

1. Berechtigtes Interesse: Der EuGH hat geprüft, ob der Sportverband ein berechtigtes Interesse daran hat, die Daten seiner Mitglieder an Sponsoren weiterzugeben. Ein berechtigtes Interesse kann viele Formen annehmen, muss aber immer sorgfältig mit den Rechten und Freiheiten der betroffenen Personen abgewogen werden.

2. Datenschutz-Grundverordnung (DSGVO): Die Entscheidung stützt sich auf die Datenschutz-Grundverordnung, insbesondere auf Artikel 6, der die Zulässigkeit der Datenverarbeitung regelt. Der EuGH stellte klar, dass die Verarbeitung personenbezogener Daten nur dann rechtens ist, wenn sie zur Verwirklichung eines berechtigten Interesses erforderlich ist und keine überwiegenden Interessen der betroffenen Person entgegenstehen.

3. Abwägung der Interessen: Der EuGH betonte, dass eine sorgfältige Abwägung zwischen den Interessen des Sportverbandes und den Datenschutzrechten der Mitglieder erforderlich ist. Diese Abwägung muss von Fall zu Fall erfolgen und alle relevanten Umstände berücksichtigen.

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

Milica Stefanovic
MLaw Rechtsanwältin[1,2]
stefanovic@fsdz.ch

Carmen de la Cruz
lic.jur.Rechtsanwältin und Notarin[1,2]
eidg. dipl. Wirtschaftsinformatikerin
sekretariat@fsdz.ch

Argonita Ameti
MLaw Juristische Mitarbeiterin
ameti@fsdz.ch

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

[1] Mitglied des Schweizerischen Anwaltsverbandes
[2] Eingetragen im Anwaltsregister des Kantons Zug

Ausdrückliche Einwilligung

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 6 Grundsätze

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

7 Die Einwilligung muss ausdrücklich erfolgen für:

a. die Bearbeitung von besonders schützenswerten Personendaten;

b. ein Profiling mit hohem Risiko durch eine private Person; oder

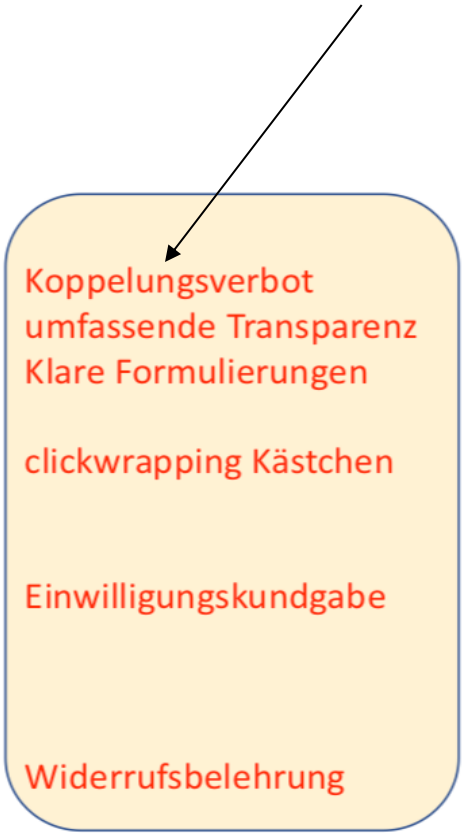
c. ein Profiling durch ein Bundesorgan.

Ausdrückliche Einwilligung

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

- **Ausdrückliche Einwilligung** ist

- jede **freiwillig** für den bestimmten Fall,
- in **informierter** Weise und
- **unmissverständlich** abgegebene Willensbekundung
- in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden **Handlung**,
- mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten **einverstanden** ist.
- Die ausdrückliche Einwilligung ist **jederzeit widerrufbar** (Betroffenenrechte –> eingeschränkte Nutzung –> Anspruch auf Löschung meiner gespeicherten und verarbeiteten personenbezogenen Daten).



Koppelungsverbot – „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

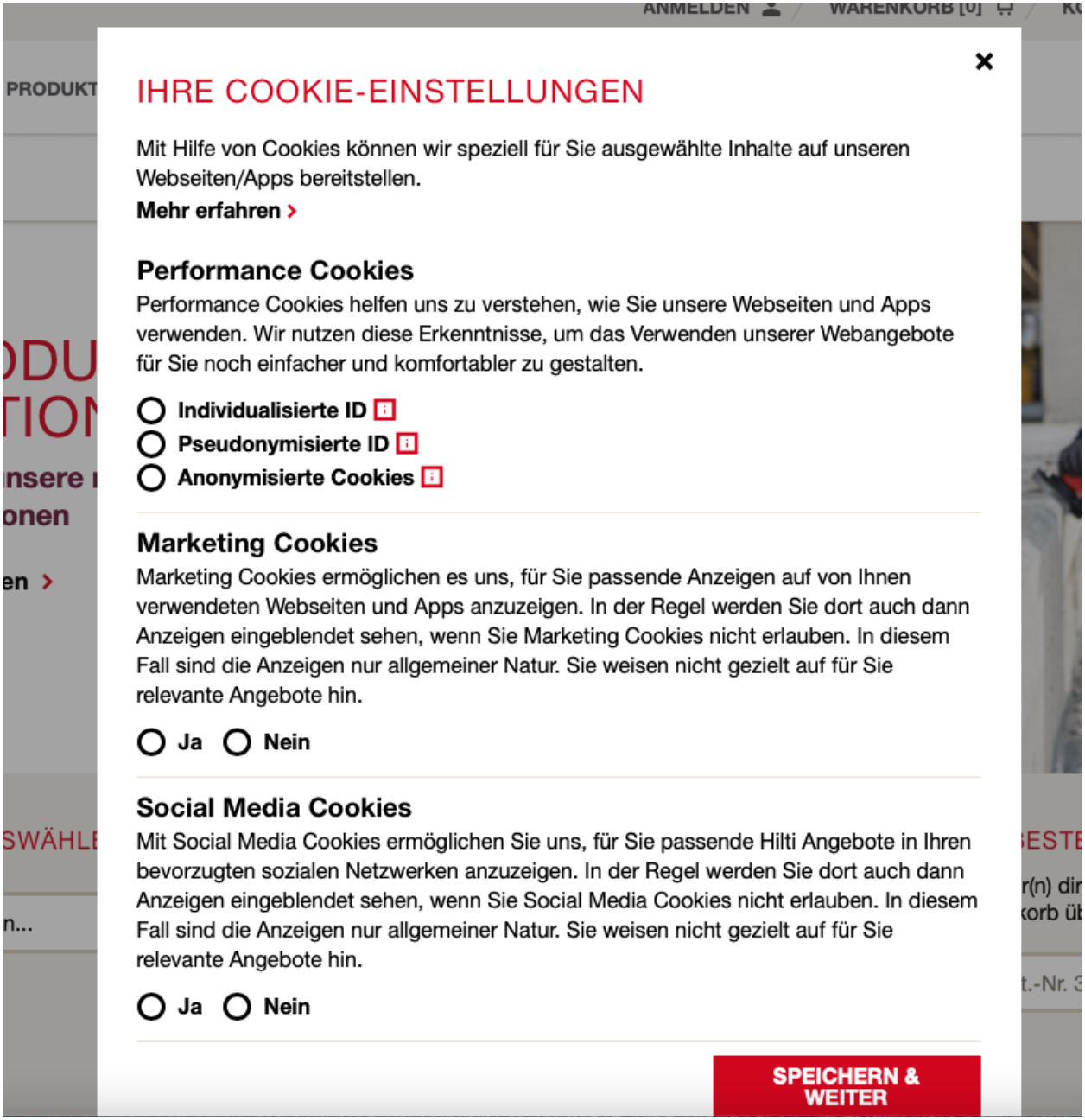
Zu den Neuprodukten >

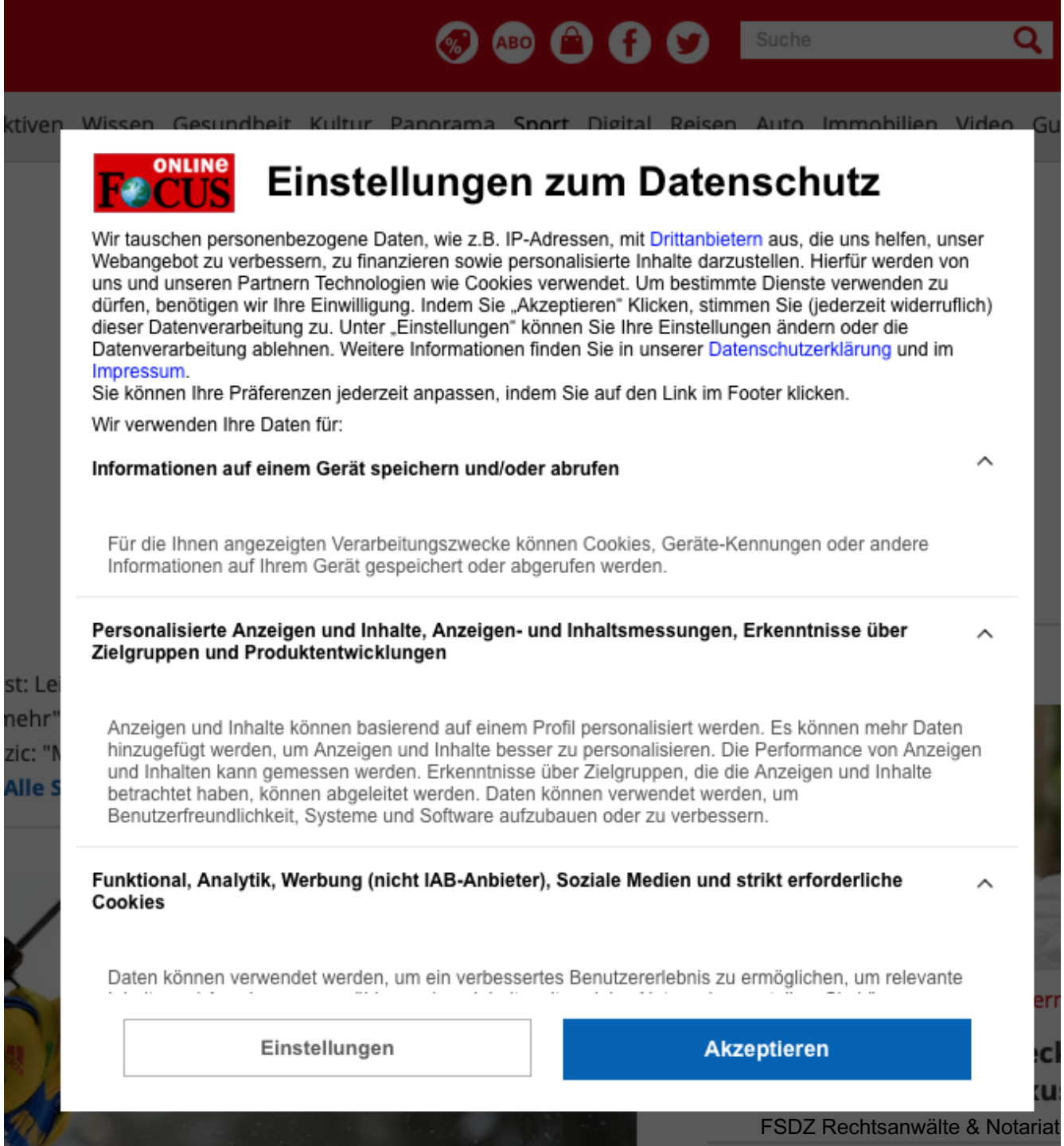
PROFITIEREN SIE VON PERSONALISIERTEN WEBANGEBOTEN - DURCH DEN GEZIELTEN EINSATZ VON COOKIES

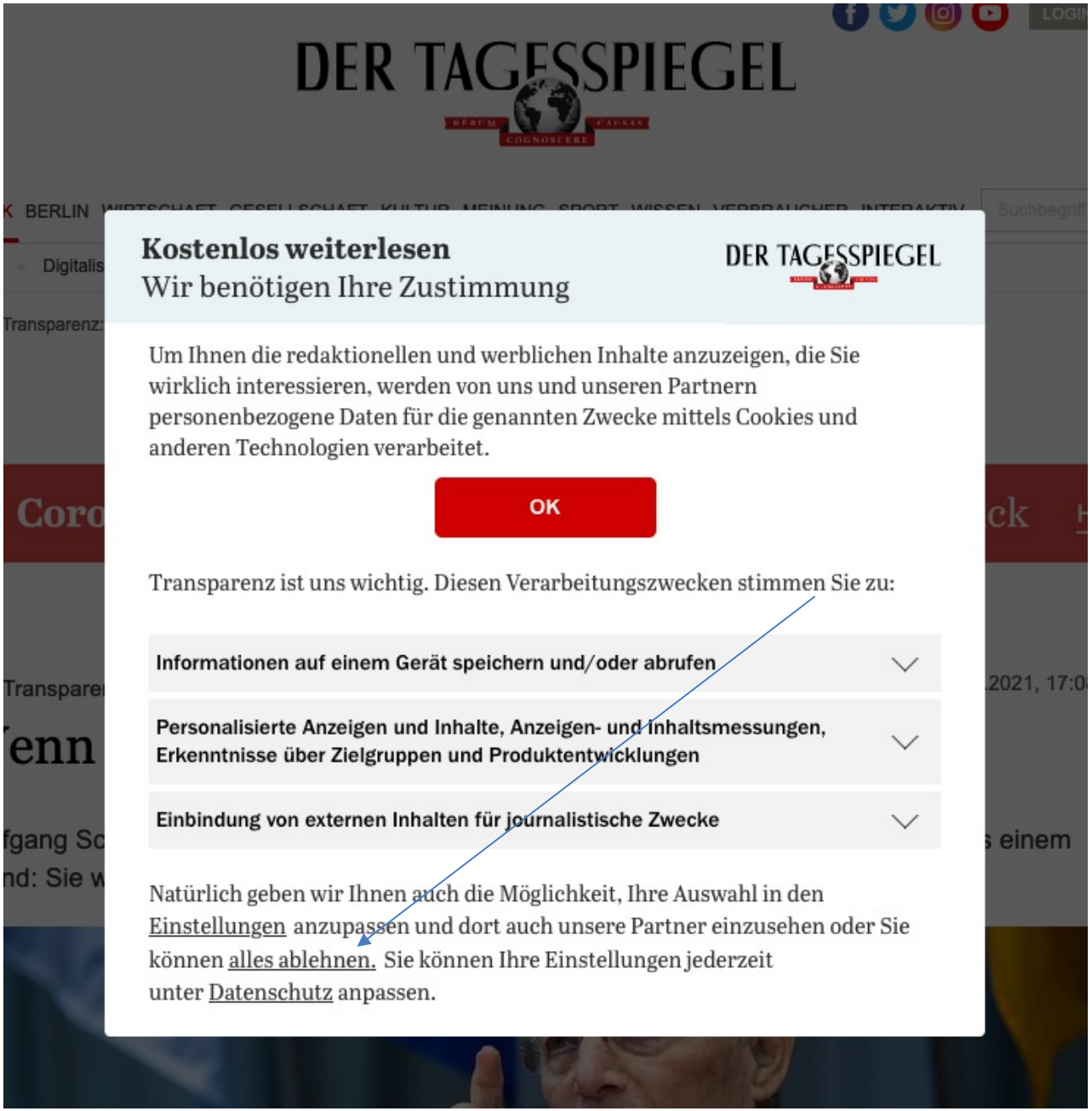
Mit Ihrer Erlaubnis nutzt Hilti Cookies, um die Verwendung unsere Webseiten/Apps einfacher und komfortabler für Sie zu machen.

COOKIE-EINSTELLUNGEN ANNEHMEN

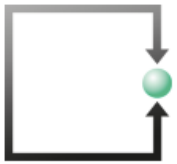
WÄHLEN SIE IHRE INDIVIDUELLEN COOKIE-EINSTELLUNGEN


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


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 (2)



Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

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

Impressum Datenschutzbestimmungen

Profil Kompetenzen Team Aktuell Publikationen Referenzen Kontakt

« Zurück zur Übersicht

Voreingestellte Einwilligung in Cookies ist unzulässig

Verfasst am 01.10.2019

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

Weiterlesen

Jetzt anrufen 041 727 60 80
oder E-Mail schreiben

FSDZ Rechtsanwälte & Notariat AG

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

Bearbeitungsgrundsätze

Rechtmässigkeit – Treu und Glauben – Verhältnismässigkeit - Zweckbestimmung

Art. 6 Grundsätze

1 Personendaten müssen rechtmässig bearbeitet werden.

2 Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein.

3 Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.

Zweckbestimmte Bearbeitung - Bearbeitungsverzeichnis

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 Kategori[illegible]offener Personen und der Kategorien bearbeiteter Personendaten

Alle weiteren Details durch Bettina Schneider

Schönes Beispiel: Evangelische Kirche Deutschland mit Merkblatt und Musterverzeichnis:
https://datenschutz.ekd.de/infothek-items/verzeichnis-der-verarbeitungstaetigkeiten/

24.4055 POSTULAT

Die Tyrannei des Datenschutzes stoppen

Eingereicht von:	 NANTERMOD PHIL FDP-Liberale Fraktio FDP.Die Liberalen
Einreichungsdatum:	26.09.2024
Eingereicht im:	Nationalrat
Stand der Beratungen:	Eingereicht

Postulat Nantermod (24.405): Die Tyrannei des Datenschutzes stoppen

Postulat Nantermod (24.405): Die Tyrannei des Datenschutzes stoppen

Eingereichter Text

Der Bundesrat wird beauftragt, im Rahmen einer rechtlichen Analyse wirksame Massnahmen für **Erleichterungen in der Datenschutzgesetzgebung** vorzulegen. Die Datenschutzbestimmungen sollen gelockert, extensive Auslegungen der Gesetzgebung verhindert und die Interventionen des Eidgenössischen Daten- schutz- und Öffentlichkeitsbeauftragten (EDÖB) bei Privaten begrenzt werden.

Begründung

Mit der Entwicklung der Informationstechnologie ist der Datenschutz zu einem wichtigen Anliegen geworden. Das Thema ist derart in den Fokus gerückt, dass sich daraus ein regelrechtes Geschäft ergeben hat. **Unzählige Beraterinnen und Berater** haben Datenschutz zu ihrem Beruf gemacht.

Es geht überhaupt nicht mehr darum, den Bürgerinnen und Bürgern den Alltag zu erleichtern und ihre Privatsphäre zu schützen. Im Gegenteil, die hohen Anforderungen an den Datenschutz erschweren die zwischenmenschlichen Beziehungen unnötig, verhindern und verkomplizieren den Zugang zu sehr praktischen Hilfsmitteln, erhöhen die Kosten für Unternehmen und schaffen eine **höllische Bürokratie**.

Während sich die eigens für Datenschutzzwecke geschaffenen Behörden an den **zahlreichen Richtlinien begeistern**, die sie produzieren, damit sich die Bürgerinnen und Bürger voreinander schützen können, haben Letztere das berechtigte Gefühl, bevormundet zu werden und die Vorteile der neuen Technologien nicht mehr ungehindert nutzen zu können.

Beispiele hierfür sind die zahlreichen Verbote, sehr praktische Anwendungen wie Whatsapp zu nutzen, die manchmal absurden Anforderungen an Unternehmen zur Beschaffung von Daten, die gar nicht vertraulich sind, oder die ewigen Cookies, die das Surfen im Internet so anstrengend machen. Vor Kurzem kündigte Apple an, einige seiner Dienste, darunter auch die praktischsten, wegen der unnötigen Gesetzgebung im Bereich Datenschutz für Nutzerinnen und Nutzer in Europa nicht mehr anzubieten. In der Schweiz intervenierte der EDÖB sogar bei der Plattform Digitec: Die Plattform habe nicht das Recht, für Bestellungen die Einrichtung eines Kundenkontos zu verlangen. **Dieser Eingriff des EDÖB in die Privatwirtschaft hat überhaupt nichts mit Datenschutz zu tun**.

Weiter sind die erwähnten neuen Datenschutzbestimmungen in einer Zeit, in der Europa und die Schweiz darauf achten müssen, wirtschaftlich nicht völlig den Anschluss zu verlieren, ein klares Innovationshemmnis. Zu guter Letzt kann man sich vor dem Hintergrund der aktuellen Ausgabenkürzungen fragen, ob im Bereich Datenschutz nicht erhebliche Einsparungen gemacht werden könnten.

Verantwortlicher

Art. 4 §7 DSGVO / Art. 5 Lit. j nDSG

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

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

Art. 5 Begriffe

In diesem Gesetz bedeuten:

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

Art. 6 Grundsätze

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

Auftragsbearbeiter (nDSG)
Auftragsverarbeiter (DSGVO)

Art. 4 §8 DSGVO / Art. 5 Lit. k und Art. 9 nDSG

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

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

Art. 5 Begriffe
In diesem Gesetz bedeuten:

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

Auslagerung der Datenbearbeitung (inkl. Cloud-Computing)

Art. 9 Bearbeitung durch Auftragsbearbeiter

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

a. die Daten so bearbeitet werden, wie der Verantwortliche selbst es tun dürfte; und

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

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

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

[4] Er kann dieselben Rechtfertigungsgründe geltend machen wie der Verantwortliche.

Art. 28 (1) DSGVO / 9 nDSG
Zusammenarbeit mit Auftragsbearbeitern

Erfolgt eine **Verarbeitung im Auftrag eines** **Verantwortlichen**,

so arbeitet dieser **nur mit** **Auftragsbearbeitern** 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 Auftragsbearbeitern

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.

bitkom

Mustervertragsanlage

Auftragsverarbeitung i. S. d. Art. 28 Abs. 3
Datenschutz-Grundverordnung (DS-GVO)
Version 1.2 (2023)

Geltungsbereich

Persönlicher & sachlicher Geltungsbereich

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;

Unternehmen sind auch private Personen

b. Bundesorgane.

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;

Kantone erlassen 26 Kantons-DSG – Kantonale Datenschutzgesetze für Kantonsverwaltungen, Gemeinden und kantonale öffentlich-rechtliche Körperschaften

Territorialer Geltungsbereich von DSGVO und nDSG

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

Angebot von Waren und Dienstleistungen

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

- Kriterium **Zielmarkt**
  AUFENTHALT der von Datenbearbeitung betroffenen Person in der EU (§ 3 Abs. 2 DSGVO)

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

Tracking – Cookies etc.

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

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.**

Teil 5:

Pflichten des Datenschutzgesetzes

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.

Bearbeitungsverzeichnis
Art. 12 nDSG

Anpassung aller Datenschutzbestimmungen auf Webseiten erforderlich

Meldepflichten

Data Breach Notifications (DSGVO)
§ 33 DSGVO und Art. 24 nDSG

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.

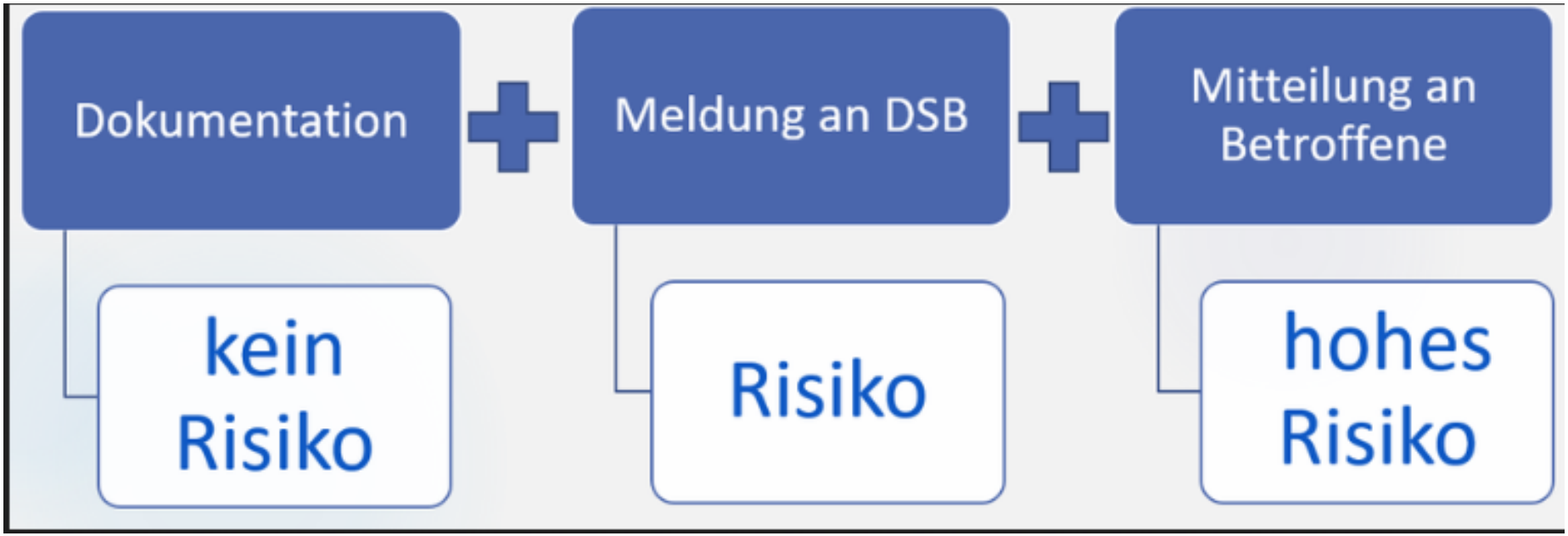
Benachrichtigung an Betroffene

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



Meldung und Benachrichtigung nach nDSG

Art. 24 Meldung von Verletzungen der Datensicherheit

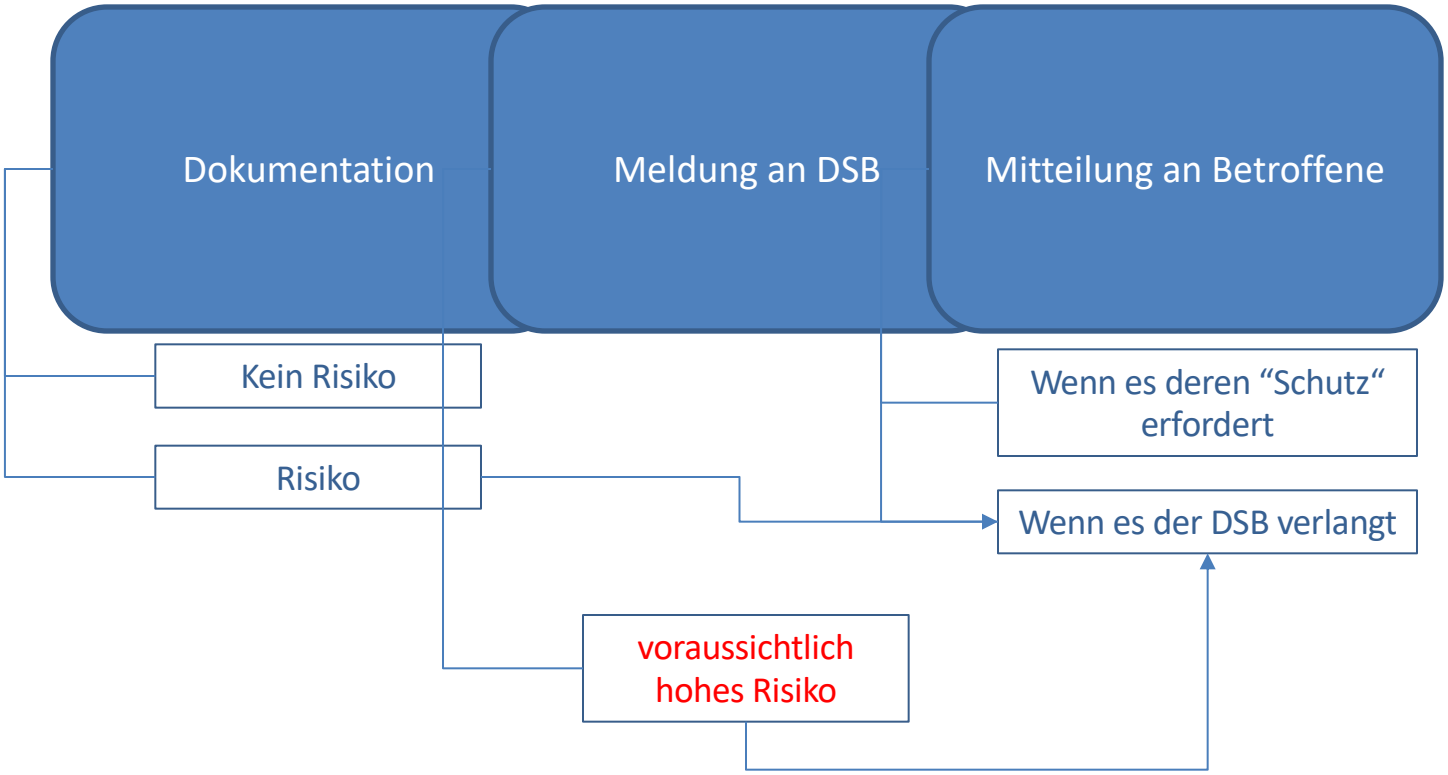
1 Der Verantwortliche meldet dem EDÖB so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

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.

Nicht direkt an Datenschutz-Aufsichtsbehörden !!

Meldung und Benachrichtigung nach nDSG



Schutzbedarf bestimmen

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;

Fokus: Schutzbedarf für die bearbeiteten Personendaten,
nicht für den Verantwortlichen oder Auftragsbearbeiter

5. Im Hinblick auf das Risiko geeignete technische & organisatorische Massnahmen (TOM‘s) festlegen

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. 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 …

Vorgängerversion VDSG

Schutzziele

Art. 2 Schutzziele

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

a. Zugriffskontrolle: Der Zugriff der berechtigten Personen ist auf diejenigen Personendaten beschränkt, die sie zur Erfüllung ihrer Aufgabe benötigen.

b. Zugangskontrolle: Der Zugang zu den Einrichtungen und Anlagen, in denen Personendaten bearbeitet werden, wird unbefugten Personen verwehrt.

c. Datenträgerkontrolle: Das Lesen, Kopieren, Verändern, Verschieben oder Entfernen von Datenträgern wird unbefugten Personen verunmöglicht.

d. Speicherkontrolle: Unbefugte Eingabe in den Datenspeicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten wird verhindert.

e. Benutzerkontrolle: Die Benutzung von automatisierten Datenbearbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen wird verhindert.

f. Transportkontrolle: Bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern wird verhindert, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature] [QR Code]

Verordnung
zum Bundesgesetz über den Datenschutz
(VDSG)

vom …

Vorgängerversion VDSG

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).

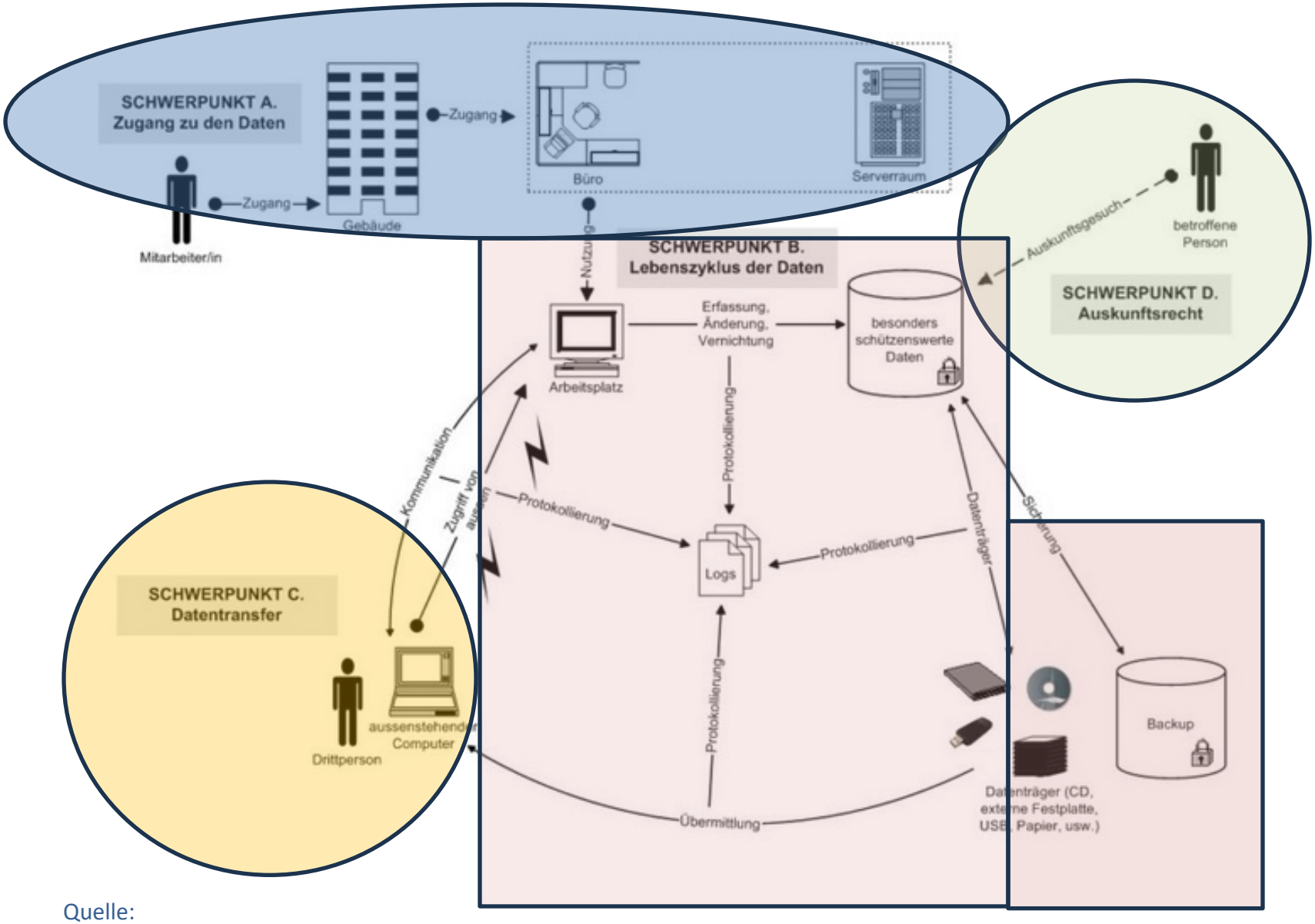
k. Erkennung: Verletzungen der Datensicherheit können rasch erkannt und Massnahmen zur Minderung oder Beseitigung der Folgen eingeleitet werden.

Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes (TOM)

- A. Zugang zu den Daten
- B. Lebenszyklus der Daten
- C. Datentransfer
- D. Auskunftsrechte

15. Januar 2024

INHALTSVERZEICHNIS



Quelle:
https://www.mll-news.com/edoeb-veroeffentlicht-leitfaden-zu-den-technischen-und-organisatorischen-massnahmen-des-datenschutzes/

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 deren Verwendung informiert.		
4.2. Setzt der Anbieter Software von Drittanbietern ein? Wenn ja welche?		
4.3. Muss allfällige Software von Drittanbietern durch separate zusätzliche Lizenz- und/oder Wartungsverträge abgesichert werden?		
4.4. Verfügt der Anbieter über die erforderlichen Nutzungs- und Vertriebsrechte an der eingesetzten Software von Drittanbietern?		
4.5. Wie stellt der Anbieter dem Kunden bei einem Ausfall des Cloudservice von mehr als 2 Werktagen konkret eine Umgehungslösung für die Sicherstellung eines fortlaufenden operativen Betriebs zur Verfügung (Ziffer 3.6. Rahmenvertrag)?		
4.6. Wie verpflichtet der Anbieter konkret seine Mitarbeitenden zur Geheimhaltung (Ziffer 5.2. Rahmenvertrag)?		
4.7. Wie verpflichtet der Anbieter konkret seine Mitarbeitenden zur Einhaltung der		

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 vorlegen?		
5.2. Wie stellt der Anbieter konkret sicher, dass Zugriffe auf Applikationen, in welchen Personendaten bearbeitet werden, protokolliert werden (Ziffer 5.12. Rahmenvertrag)? Wie sehen die konkreten Überwachungsdaten aus, die der Anbieter dem Kunden zur Verfügung stellen kann?		
5.3. Der Anbieter zeigt auf, welche anerkannten Methoden und aktuellen Standards er im Zusammenhang mit der vertragsgemässen Erfüllung im Bereich Datenschutz und Datensicherheit konkret anwendet (Ziffer 6.4 Rahmenvertrag)?		
5.4. Wie stellt der Anbieter konkret sicher, dass nur berechtigte Personen auf die		

20 Massnahmenvorschläge

https://www.fsdz.ch/file-docs/selbstdeklaration.pdf

Spezialvorschrift in der DSGVO

Datenschutz-Vertreter nach Art. 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

Vertretung in der Schweiz

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. 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.

Teil 6:

Sanktionen

Sanktionen in der DSGVO

Sanktionen

Aufsichtsbehörden in EU-Ländern

- **Direktes Sanktionierungsrecht** gegenüber UN
- Katalog von Sanktionen (Art. 58 § 2 DSGVO)

  - Mahnung
  - Verwarnung
  - Förmliche Bekanntmachung der UN und des Verstosses
  - Vorübergehende Beschränkung der Datenbearbeitung
  - Dauerhafte Beschränkung der Datenbearbeitung
  - **Geldbussen** von bis zu € 20 Mio oder 4% des weltweiten Jahresumsatzes
  - Weitergehender Schaden (Schadenersatz und Zinsen) aus einem Gerichtsverfahren bleibt zusätzlich vorbehalten.

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

URTEIL DES EUROPÄISCHEN GERICHTSHOFS EuGH
vom 5. Dezember 2023 (C-807/21)

Kammergericht, Urteil vom 22. Januar 2024 - 3 - Ws 250/21, 161 AR 84/21, 3

1. Die in Art. 83 DSG-VO vorgesehenen Geldbussen können **unmittelbar gegen juristische Personen** verhängt werden, wenn diese als für die Datenbearbeitung Verantwortliche einzustufen sind.

2. Es ist weder ein Verschulden eines Repräsentanten noch einer Aufsichtspflichtverletzung erforderlich. Vielmehr sind **Unternehmen im Deliktsbereich der DSG-VO per se schuldfähig**.

3. Nationale Bestimmungen, die einen anderen Ansatz vorsehen (nur natürliche Personen seien schuldfähig), werden durch die Bestimmungen der DSG-VO übersteuert (und sind nicht gültig).

4. Der **Bussgeldentscheid muss die natürliche Person**, der eine Pflichtverletzung zur Last fällt, **nicht bezeichnen**.

Sanktionen im CH-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

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[tz]
über den D[aten]schutz
(Datenschutz[ge]tz, DSG)

vom 25. Septem[ber] 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 EDOB 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

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. 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.

Teil 7:

Betroffenenrechte

Recht auf Auskunft

4. Kapitel: Rechte der betroffenen Person

Art. 25 Auskunftsrecht

1 Jede Person kann vom Verantwortlichen Auskunft darüber verlangen, ob Personendaten über sie bearbeitet werden.

Recht auf Auskunft

3. Kapitel: Rechte der betroffenen Person

1. Abschnitt: Auskunftsrecht

Art. 16 Modalitäten

[1] Wer vom Verantwortlichen Auskunft darüber verlangt, ob Personendaten über sie oder ihn bearbeitet werden, muss dies schriftlich tun. Ist der Verantwortliche einverstanden, so kann das Begehren auch mündlich mitgeteilt werden.

[2] Die Auskunftserteilung erfolgt schriftlich oder in der Form, in der die Daten vorliegen. Im Einvernehmen mit dem Verantwortlichen kann die betroffene Person ihre Daten an Ort und Stelle einsehen. Die Auskunft kann mündlich erteilt werden, wenn die betroffene Person einverstanden ist.

[3] Das Auskunftsbegehren und die Auskunftserteilung können auf elektronischem Weg erfolgen.

[4] Die Auskunft muss der betroffenen Person in einer verständlichen Form erteilt werden.

[5] Der Verantwortliche muss angemessene Massnahmen treffen, um die betroffene Person zu identifizieren. Diese ist zur Mitwirkung verpflichtet.

Recht auf Auskunft

Art. 18 Frist

[1] Die Auskunft muss innerhalb von 30 Tagen seit dem Eingang des Begehrens erteilt werden.

[2] Kann die Auskunft nicht innerhalb von 30 Tagen erteilt werden, so muss der Verantwortliche die betroffene Person darüber informieren und ihr mitteilen, innerhalb welcher Frist die Auskunft erfolgt.

[3] Verweigert der Verantwortliche die Auskunft, schränkt er sie ein oder schiebt er sie auf, so muss er dies innerhalb derselben Frist mitteilen.

Recht auf Berichtigung

Art. 32 Rechtsansprüche

[1] Die betroffene Person kann verlangen, dass unrichtige Personendaten berichtigt werden, es sei denn:

a. eine gesetzliche Vorschrift verbietet die Änderung;

b. die Personendaten werden zu Archivzwecken im öffentlichen Interesse bearbeitet.

Recht auf Datenherausgabe und Übertragung

Art. 28 Recht auf Datenherausgabe oder -übertragung

1 Jede Person kann vom Verantwortlichen die Herausgabe ihrer Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen, wenn:

a. der Verantwortliche die Daten automatisiert bearbeitet; und

b. die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden.

2 Die betroffene Person kann zudem vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen überträgt, wenn die Voraussetzungen nach Absatz 1 erfüllt sind und dies keinen unverhältnismässigen Aufwand erfordert.

Recht auf Datenherausgabe und Übertragung

Art. 21 **Technische Anforderungen an die Umsetzung**

[1] Als gängiges elektronisches Format gelten Formate, die es ermöglichen, dass die Personendaten mit verhältnismässigem Aufwand übertragen und von der betroffenen Person oder einem anderen Verantwortlichen weiterverwendet werden.

[2] Das Recht auf Datenherausgabe oder -übertragung begründet für den Verantwortlichen nicht die Pflicht, technisch kompatible Datenbearbeitungssysteme zu übernehmen oder beizubehalten.

[3] Ein unverhältnismässiger Aufwand für die Übertragung von Personendaten auf einen anderen Verantwortlichen liegt vor, wenn die Übertragung technisch nicht möglich ist.

Übrige Ansprüche

[2] Klagen zum Schutz der Persönlichkeit richten sich nach den Artikeln 28, 28*a* sowie 28*g*–28*l* des Zivilgesetzbuchs[7]. Die klagende Partei kann insbesondere verlangen, dass:

a. eine bestimmte Datenbearbeitung verboten wird;

b. eine bestimmte Bekanntgabe von Personendaten an Dritte untersagt wird;

c. Personendaten gelöscht oder vernichtet werden.

[3] Kann weder die Richtigkeit noch die Unrichtigkeit der betreffenden Personendaten festgestellt werden, so kann die klagende Partei verlangen, dass ein Bestreitungsvermerk angebracht wird.

[4] Die klagende Partei kann zudem verlangen, dass die Berichtigung, die Löschung oder die Vernichtung, das Verbot der Bearbeitung oder der Bekanntgabe an Dritte, der Bestreitungsvermerk oder das Urteil Dritten mitgeteilt oder veröffentlicht wird.

1. Verbot der Datenbearbeitung
2. Bekanntgabe an Dritte untersagen
3. Personendaten löschen
4. Personendaten vernichtet

Spezialbestimmungen des CH-nDSG

Verhaltenskodex und Zertifizierungsverfahren

Verhaltenskodizes und Zertifizierungsverfahren

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.

Verordnung über Datenschutzzertifizierungen
(VDSZ)

vom 31. August 2022

[2] Je eine separate Akkreditierung ist erforderlich für die Zertifizierung:

a. der Organisation und der Verfahren (Managementsysteme) im Zusammenhang mit Datenbearbeitungen;

b. von Produkten, namentlich Datenbearbeitungssystemen oder -programmen und Hardware, sowie von Dienstleistungen und Prozessen im Zusammenhang mit Datenbearbeitungen.

Teil 8:

Cloud-Computing und Bearbeitung und Speicherung von Informationen im Ausland

Bekanntgabe Personendaten ins Ausland

3. Abschnitt: Bekanntgabe von Personendaten ins Ausland

Art. 16 Grundsätze

[1] Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

[2] Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:

a. einen völkerrechtlichen Vertrag;

b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden;

c. spezifische Garantien, die das zuständige Bundesorgan erarbeitet und dem EDÖB vorgängig mitgeteilt hat;

d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat; oder

e. verbindliche unternehmensinterne Datenschutzvorschriften, die vorgängig vom EDÖB oder von einer für den Datenschutz zuständigen Behörde eines Staates, der einen angemessenen Schutz gewährleistet, genehmigt wurden.

[3] Der Bundesrat kann andere geeignete Garantien im Sinne von Absatz 2 vorsehen.

Bekanntgabe Personendaten ins Ausland

Art. 17 Ausnahmen

[1] Abweichend von Artikel 16 Absätze 1 und 2 dürfen in den folgenden Fällen Personendaten ins Ausland bekanntgegeben werden:

a. Die betroffene Person hat ausdrücklich in die Bekanntgabe eingewilligt.

b. Die Bekanntgabe steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags:
   1. zwischen dem Verantwortlichen und der betroffenen Person; oder
   2. zwischen dem Verantwortlichen und seiner Vertragspartnerin oder seinem Vertragspartner im Interesse der betroffenen Person.

c. Die Bekanntgabe ist notwendig für:
   1. die Wahrung eines überwiegenden öffentlichen Interesses; oder
   2. die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor einem Gericht oder einer anderen zuständigen ausländischen Behörde.

d. Die Bekanntgabe ist notwendig, um das Leben oder die körperliche Unversehrtheit der betroffenen Person oder eines Dritten zu schützen, und es ist nicht möglich, innerhalb einer angemessenen Frist die Einwilligung der betroffenen Person einzuholen.

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.

← Zurück zur Übersicht

Digitale Basisdienste: Mit Neuerlass Rechtsgrundlagen schaffen

Mitteilung 13.02.2024

Bevölkerung und Unternehmen sollen ihre Rechte und Pflichten einfach, durchgängig und sicher auf dem elektronischen Weg wahrnehmen können (RRB Nr. 1362/2021). Digitale Basisdienste bilden wichtige Komponenten der digitalen Verwaltung. Damit das digitale Leistungsangebot der Verwaltung weiter ausgebaut werden kann, sind neue Rechtsgrundlagen erforderlich. Der Regierungsrat hat die Staatskanzlei ermächtigt, das Vernehmlassungsverfahren zum Gesetz über digitale Basisdienste durchzuführen.

Vernehmlassung
13.2.2024 bis 13. Mai 2024

Vorentwurf

C. Digitaler Arbeitsplatz

Informationsbearbeitung durch Dritte im Rahmen des digitalen Arbeitsplatzes

§ 17. [1] Das öffentliche Organ kann die Bearbeitung von Informationen in Anwendungen des digitalen Arbeitsplatzes an Anbieterinnen von cloudbasierten Informatikdienstleistungen übertragen, wenn sich deren Rechenzentren in der Schweiz oder in der Europäischen Union befinden, und wenn:

a. das öffentliche Organ besondere Personendaten sowie vertrauliche oder der Geheimhaltung unterliegende Informationen auch gegenüber der Cloud-Anbieterin wirksam verschlüsselt, so dass die Cloud-Anbieterin darauf nicht ohne Mitwirkung des öffentlichen Organs zugreifen kann und

b. das öffentliche Organ die sonstigen Informationen durch alle zumutbaren organisatorischen, technischen und vertraglichen Massnahmen schützt und das verbleibende Risiko einer Bekanntgabe insbesondere angesichts der Bedeutung der Informationen, des Zwecks und der Art und Weise ihrer Bearbeitung sowie der Grundrechte der betroffenen Personen vertretbar ist.

[2] Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz.

Besondere Personendaten und vertrauliche und geheimzuhaltende Informationen:

Verschlüsselung: Entschlüsselung **nicht ohne Mitwirkung des öffentlichen Organs**

Sonstige Informationen:

- **angemessene TOM's** und
- **Restrisiktobeurteilung** (Abwägung)

Kt. ZH: Gesetz über digitale Basisdienste- Entwurf des Regierungsrats ohne Cloudverbot

10. Oktober 2024

Der Kanton Zürich hatte eine Vernehmlassung zum "Gesetz über digitale Basisdienste" durchgeführt (siehe hier). Neben weiteren Punkten sah § 17 in der damals vorgeschlagenen Fassung vor, dass Informationen grundsätzlich in der Schweiz oder der EU zu speichern sind, und bei besonderen Personendaten bzw. vertraulichen oder geheimen Daten eine Verschlüsselung erforderlich ist, die einen Zugriff ohne Mitwirkung des öffentlichen Organs auch dem Cloud-Provider verunmöglicht – das hätte im Wesentlichen noch Hostingdienste erlaubt.

In der Vernehmlassung ist dieser Punkt denn auch auf scharfe Kritik gestossen, die im Bericht des Regierungsrats wie folgt zusammengefasst wird:

> Kontrovers diskutiert wurde in der Vernehmlassung der Regelungsvorschlag zur Nutzung von cloudbasierten Applikationen im Rahmen von digitalen Arbeitsplätzen. Die Mehrheit der Vernehmlassungsteilnehmenden beantragte eine **Anpassung der Voraussetzungen oder den Verzicht** auf die Bestimmung. Vereinzelt wurde das Verhältnis zum Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG, LS 170.4) und zum Gesetz über die Auslagerung von Informatikdienstleistungen thematisiert. [...]

Der Zürcher Regierungsrat hat dem Kantonsrat nun – am 18. September 2024 – eine geänderte Fassung des Entwurfs übergeben. In der neuen Fassung liest sich § 17 wie folgt:

> § 17. 1 Das Bearbeiten von **Personendaten und besonderen Personendaten** in Applikationen digitaler Arbeitsplätze der Behörden kann an Dritte übertragen werden, wenn
>
> a. sich deren Rechenzentren in der Schweiz oder in einem Staat mit einem angemessenen Datenschutz befinden und
>
> b. aufgrund der getroffenen technischen, organisatorischen und vertraglichen Massnahmen **kein Grund zur Annahme besteht**, dass ein ausländischer Staat auf die Daten **zugreifen wird**.
>
> 2 Im Übrigen gelten die Bestimmungen des Gesetzes über die Information und den Datenschutz vom 12. Februar 2007*.

Das entspricht im Wesentlichen den Vorgaben des **§ 36** im Entwurf des revidierten IDG Zürichs. Eine Bekanntgabe von Personendaten ins Ausland ist danach – neben den übrigen Voraussetzungen der Datenbearbeitung – erlaubt, wenn

> b. im Empfängerstaat ein angemessener Schutz für die Datenbearbeitung gewährleistet ist oder
>
> c. [das öffentliche Organ] mit den Empfängerinnen und Empfängern angemessene Sicherheitsvorkehrungen vereinbart hat.

https://datenrecht.ch/kt-zh-gesetz-ueber-digitale-basisdienste-entwurf-des-regierungsrats-ohne-cloudverbot/?utm_source=datenrecht&utm_campaign=8f090b79fd-datenrecht-Mailchimp&utm_medium=email&utm_term=0_15155ce73b-8f090b79fd-90792857

RRB-2024-427

Ergänzung der eGovernment- und Informatik-Strategie 2021; Einsatz von Cloud Computing im Informatik-Grundbedarf und Einführung Microsoft 365 Cloud-Dienste; Genehmigung

G. Beschluss des Regierungsrates

1. Die Ergänzung der eGovernment- und Informatik-Strategie 2021 bezüglich des Einsatzes von Cloud Computing im Informatik-Grundbedarf wird genehmigt. Die Informatikstrategie-Kommission wird eingeladen, das Genehmigungsverfahren bei den Gemeinden durchzuführen.

2. Die Einführung von Microsoft 365 Cloud-Diensten in Kanton und Gemeinden wird, vorbehältlich der Genehmigung der Strategie-Ergänzung durch die Gemeinden, bewilligt. Die Nutzung erfolgt unter den in den Erwägungen ausgeführten Rahmenbedingungen.

3. Das Departement Finanzen wird beauftragt, in Zusammenarbeit mit der Kantonskanzlei, dem Datenschutz-Kontrollorgan und der AR Informatik AG einheitliche und verbindliche Weisungen für die Nutzung von M365 Cloud-Diensten auszuarbeiten, die Gemeinden dazu anzuhören und dem Regierungsrat zur Genehmigung zu unterbreiten.

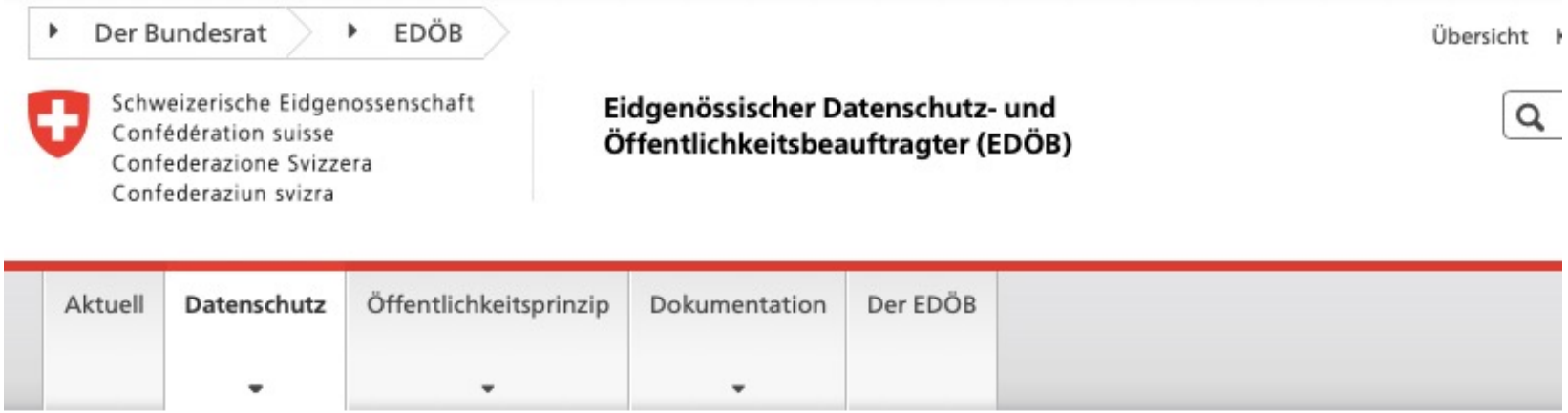
4. Die AR Informatik AG wird beauftragt, eine Exit-Strategie zu erarbeiten.

Auszug an

Departement Finanzen
Kantonskanzlei
Informatikstrategie-Kommission
AR Informatik AG
Datenschutz-Kontrollorgan (mit Beilage 2)

Im Auftrag des Regierungsrates:

Roger Nobs, Ratschreiber


Der Bundesrat
EDÖB
Übersicht
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)
Aktuell
Datenschutz
Öffentlichkeitsprinzip
Dokumentation
Der EDÖB
Startseite › Datenschutz › Handel und Wirtschaft › Übermittlung ins Ausland
Handel und Wirtschaft
Übermittlung ins Ausland
USA - Privacy Shield
Outsourcing
Datenweitergabe an ausländische Behörden
Übermittlung ins Ausland
Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug
Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge
Standardvertragsklauseln (SCC)
Weitere Informationen
Das schweizerische Datenschutzgesetz gewährleistet den Schutz der Privatsphäre für Datenbearbeitungen, die von Personen in der

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 16 Abs. 2 lit. b und d DSG)

(veröffentlicht Juni 2021; angepasst an das revidierte DSG Mai 2023)

1. Zweck der Anleitung

Die vorliegende Anleitung soll Datenbearbeitern die Prüfung der Zulässigkeit von Datenübermittlungen von personenbezogenen Daten ins Ausland erleichtern.

Anhand eines Schemas erläutert diese Anleitung den Anwendungsfall des Datentransfers ins Ausland nach Art. 16 Abs. 2 lit. b DSG, wenn dort eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet, und dieser Mangel durch Datenschutzklauseln in einem Vertrag oder Standarddatenschutzklauseln kompensiert werden muss (vgl. auch Art. 9 Abs. 3 der Verordnung zum Bundesgesetz über den Datenschutz DSV, vom 31. August 2022 , SR. 235.11). Auf die Voraussetzungen nach lit. a, c und e und Art. 17 wird in dieser Anleitung nicht eingegangen.

Beilage in den Unterlagen

Verordnung über den Datenschutz
(Datenschutzverordnung, DSV)

Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge

27. August 2021

vom 31. August 2022 (Stand am 1. Januar 2024)

Art. 8

Beurteilung der Angemessenheit des Datenschutzes eines Staates, eines Gebiets, eines spezifischen Sektors in einem Staat oder eines internationalen Organs

[1] Die Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz werden in Anhang 1 aufgeführt.

Anhang 1
(Art. 8 Abs. 1)

Staaten, Gebiete, spezifische Sektoren in einem Staat und internationale Organe mit einem angemessenen Datenschutz

1	Deutschland*
2	Andorra***
3	Argentinien***
4	Österreich*
5	Belgien*
6	Bulgarien***
8	Zypern***
9	Kroatien***
10	Dänemark*
11	Spanien*
12	Estland*
13	Finnland*
14	Frankreich*
15	Gibraltar***
16	Griechenland*
17	Guernsey***
18	Ungarn*
19	Isle of Man***
20	Färöer***
21	Irland***
22	Island*
23	Israel***
24	Italien*
25	Jersey***
26	Lettland*
27	Liechtenstein*
28	Litauen*
29	Luxemburg*
30	Malta*
31	Monaco***
32	Norwegen*
33	Neuseeland***
34	Niederlande*
35	Polen*
36	Portugal*
37	Tschechien*
38	Rumänien***
39	Vereinigtes Königreich**

* Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten nach der Richtlinie (EU) 2016/680[7] mit ein.

** Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten gemäss einem Durchführungsbeschluss der Europäischen Kommission, mit welchem die Angemessenheit des Datenschutzes nach der Richtlinie (EU) 2016/680 festgestellt wird, mit ein.

*** Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten im Rahmen der von der Richtlinie (EU) 2016/680 vorgesehenen Zusammenarbeit nicht mit ein.

https://www.fedlex.admin.ch/eli/cc/2022/568/de

SCC - Standard Contractual Clauses der EU

ANHANG I

A. **LISTE DER PARTEIEN**

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Datenexporteur(e): [*Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihres Datenschutzbeauftragten und/oder Vertreters in der Europäischen Union*]

1. Name: .....

   Anschrift: .....

   Name, Funktion und Kontaktdaten der Kontaktperson: .....

   Tätigkeiten, die für die gemäß diesen Klauseln übermittelten Daten von Belang sind: .....

   Unterschrift und Datum: .....

   Rolle (Verantwortlicher/Auftragsverarbeiter): .....

2. .....

Datenimporteur(e): [*Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson*]

1. Name: .....

   Anschrift: .....

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf anerkannte Standardvertragsklauseln und Musterverträge

27. August 2021

https://www.google.ch/search?q=ed%C3%B6b%C2%A0%C3%BCbermittlung+von+personendaten+ins+ausland&sca_esv=12ce420749b4de42&source=hp&ei=pDknZ5OqFdju7_UPtL2JgAg&iflsig=AL9hbdgAAAAAZydHtIInKOF_p1vHnnLIUDi6ZO6mk7Ot&ved=0ahUKEwiTjLC65L-JAxVY97sIHbReAoAQ4dUDCA8&uact=5&oq=ed%C3%B6b%C2%A0%C3%BCbermittlung+von+personendaten+ins+ausland&gs_lp=Egdnd3Mtd2l6IjJlZMO2YsKgw7xiZXJtaXR0bHVuZyB2b24gcGVyc29uZW5kYXRlbiBpbnMgYXVzbGFuZDIFECEYoAFI-9YBUABYxNMBcAJ4AJABAJgBsQGgAY4aqgEENDYuM7gBA8gBAPgBAZgCM6ACtx3CAgsQABiABBixAxiDAcICDhAuGIAEGLEDGNEDGMcBwgIOEAAYgAQYsQMYgwEYigXCAgsQLhiABBjRAxjHAcICDhAuGIAEGLEDGMcBGK8BwgIOEC4YgAQYsQMYgwEYigXCAgsQLhiABBjHARivAcICCBAuGIAEGLEDwgIREC4YgAQYsQMYgwEYxwEYrwHCAggQABiABBixA8ICCxAuGIAEGLEDGNQCwgILEC4YgAQYsQMYgwHCAggQLhiABBjUAsICBRAAGIAEwgIFEC4YgATCAgYQABgWGB7CAggQABiABBiiBMICCBAAGKIEGIkFwgIEECEYFcICBxAhGKABGArCAgUQIRifBZgDAJIHBjQ3LjMuMaAH468B&sclient=gws-wiz

Anleitung für die Prüfung der Zulässigkeit von Datenübermittlungen mit Auslandbezug (nach Art. 16 Abs. 2 lit. b und d DSG)

(veröffentlicht Juni 2021; angepasst an das revidierte DSG Mai 2023)

1. Zweck der Anleitung

Die vorliegende Anleitung soll Datenbearbeitern die Prüfung der Zulässigkeit von Datenübermittlungen von personenbezogenen Daten ins Ausland erleichtern.

Anhand eines Schemas erläutert diese Anleitung den Anwendungsfall des Datentransfers ins Ausland nach Art. 16 Abs. 2 lit. b DSG, wenn dort eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet, und dieser Mangel durch Datenschutzklauseln in einem Vertrag oder Standarddatenschutzklauseln kompensiert werden muss (vgl. auch Art. 9 Abs. 3 der Verordnung zum Bundesgesetz über den Datenschutz DSV, vom 31. August 2022 , SR. 235.11). Auf die Voraussetzungen nach lit. a, c und e und Art. 17 wird in dieser Anleitung nicht eingegangen.

SR 235.1 Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG), Art. 16 Abs. 1, Abs. 2 Bst. b und d

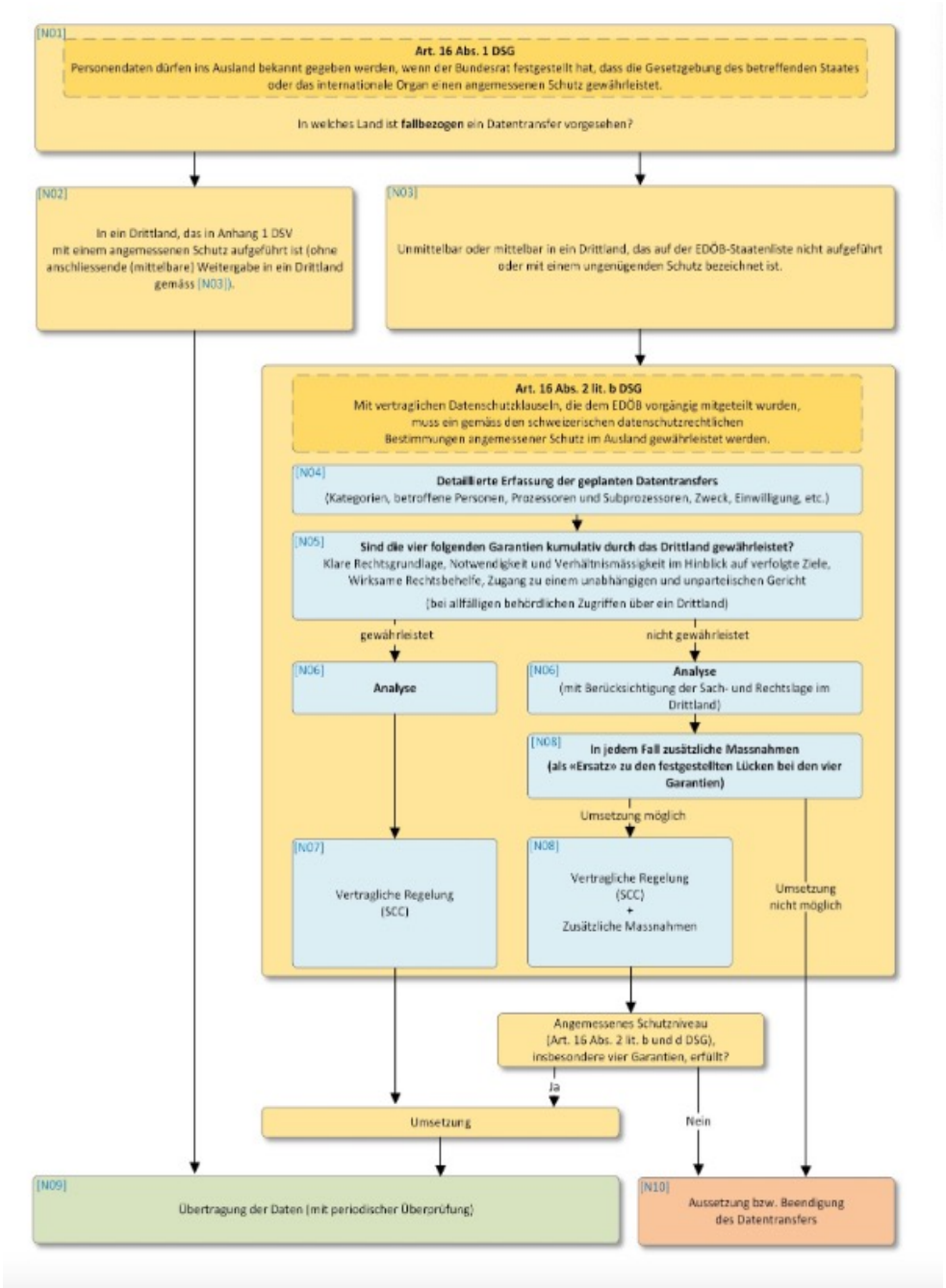
3. Abschnitt: Bekanntgabe von Personendaten ins Ausland
Art. 16 Grundsätze

1 Personendaten dürfen ins Ausland bekanntgegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.

2 Liegt kein Entscheid des Bundesrates nach Absatz 1 vor, so dürfen Personendaten ins Ausland bekanntgegeben werden, wenn ein geeigneter Datenschutz gewährleistet wird durch:
[…]
b. Datenschutzklauseln in einem Vertrag zwischen dem Verantwortlichen oder dem Auftragsbearbeiter und seiner Vertragspartnerin oder seinem Vertragspartner, die dem EDÖB vorgängig mitgeteilt wurden;
[…]
d. Standarddatenschutzklauseln, die der EDÖB vorgängig genehmigt, ausgestellt oder anerkannt hat;
[…]

SR 235.11 Verordnung vom 31. August 2022 zum Bundesgesetz über den Datenschutz (DSV), Art. 9
Art. 9 Datenschutzklauseln und spezifische Garantien

1 Die Datenschutzklauseln in einem Vertrag nach Artikel 16 Absatz 2 Buchstabe b DSG und die spezifischen Garantien nach Artikel 16 Absatz 2 Buchstabe c DSG müssen mindestens die folgenden Punkte enthalten:
a. die Anwendung der Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, der Transparenz, der Zweckbindung und der Richtigkeit;
b. die Kategorien der bekanntgegebenen Personendaten sowie der betroffenen Personen;
c. die Art und den Zweck der Bekanntgabe von Personendaten;
d. gegebenenfalls die Namen der Staaten oder internationalen Organe, in die oder denen Personendaten bekanntgegeben werden, sowie die Anforderungen an die Bekanntgabe;
e. die Anforderungen an die Aufbewahrung, die Löschung und die Vernichtung von Personendaten;
f. die Empfängerinnen und Empfänger oder die Kategorien der Empfängerinnen und Empfänger;
g. die Massnahmen zur Gewährleistung der Datensicherheit;
h. die Pflicht, Verletzungen der Datensicherheit zu melden;
i. falls die Empfängerinnen und Empfänger Verantwortliche sind: die Pflicht, die betroffenen Personen über die Bearbeitung zu informieren;
j. die Rechte der betroffenen Person, insbesondere:


[N01]
Art. 16 Abs. 1 DSG
Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates oder das internationale Organ einen angemessenen Schutz gewährleistet.
In welches Land ist fallbezogen ein Datentransfer vorgesehen?
[N02]
In ein Drittland, das in Anhang 1 DSV mit einem angemessenen Schutz aufgeführt ist (ohne anschliessende (mittelbare) Weitergabe in ein Drittland gemäss [N03]).
[N03]
Unmittelbar oder mittelbar in ein Drittland, das auf der EDÖB-Staatenliste nicht aufgeführt oder mit einem ungenügenden Schutz bezeichnet ist.
Art. 16 Abs. 2 lit. b DSG
Mit vertraglichen Datenschutzklauseln, die dem EDÖB vorgängig mitgeteilt wurden, muss ein gemäss den schweizerischen datenschutzrechtlichen Bestimmungen angemessener Schutz im Ausland gewährleistet werden.
[N04]
Detaillierte Erfassung der geplanten Datentransfers
(Kategorien, betroffene Personen, Prozessoren und Subprozessoren, Zweck, Einwilligung, etc.)
[N05]
Sind die vier folgenden Garantien kumulativ durch das Drittland gewährleistet?
Klare Rechtsgrundlage, Notwendigkeit und Verhältnismässigkeit im Hinblick auf verfolgte Ziele, Wirksame Rechtsbehelfe, Zugang zu einem unabhängigen und unparteiischen Gericht
(bei allfälligen behördlichen Zugriffen über ein Drittland)
gewährleistet
nicht gewährleistet
[N06]
Analyse
[N06]
Analyse
(mit Berücksichtigung der Sach- und Rechtslage im Drittland)
[N08]
In jedem Fall zusätzliche Massnahmen
(als «Ersatz» zu den festgestellten Lücken bei den vier Garantien)
Umsetzung möglich
[N07]
Vertragliche Regelung
(SCC)
[N08]
Vertragliche Regelung
(SCC)
+
Zusätzliche Massnahmen
Umsetzung nicht möglich
Angemessenes Schutzniveau
(Art. 16 Abs. 2 lit. b und d DSG), insbesondere vier Garantien, erfüllt?
Ja
Nein
Umsetzung
[N09]
Übertragung der Daten (mit periodischer Überprüfung)
[N10]
Aussetzung bzw. Beendigung des Datentransfers

MARCH 25, 2022

FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework

The United States and the European Commission have committed to a new Trans-Atlantic Data Privacy Framework, which will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union when it struck down in 2020 the Commission's adequacy decision underlying the EU-U.S. Privacy Shield framework.

This Framework will reestablish an important legal mechanism for transfers of EU personal data to the United States. The United States has committed to implement new safeguards to ensure that signals intelligence activities are necessary and proportionate in the pursuit of defined national security objectives, which will ensure the privacy of EU personal data and to create a new mechanism for EU individuals to seek redress if they believe they are

Microsoft: Amendmend-Vorschlag zu SIK-Rahmenverträgen mit öffentlichen Verwaltungen der Schweiz

Ungeachtet gegenteiliger Bestimmungen wird der Abschnitt "Offenlegung verarbeiteter Daten" des Datenschutznachtrag zu den Produkten und Services von Microsoft wie folgt geändert:

> In allen Fällen hält sich Microsoft ohne Ausnahme an das EU/EFTA-Recht, falls Microsoft einen rechtlichen Antrag für verarbeitete Daten von einer Nicht-EU/EFTA-Regierungsbehörde erhält.

Mit Ausnahme der durch diese Zusatzvereinbarung eingetretenen Änderungen bleibt der oben genannte Beitritt oder Vertrag unverändert und in voller Rechtskraft. Wenn ein Konflikt zwischen einer Bestimmung in dieser Zusatzvereinbarung und einer Bestimmung im oben genannten Beitritt oder Vertrag besteht, so ist diese Zusatzvereinbarung maßgebend.

Erste Reaktionen

Die EU-Kommission kann nun einen neuen Angemessenheitsbeschluss nach Art. 45 DSGVO in die Wege leiten. Die Mitgliedstaaten und der europäische Datenschutzausschusses (ADSA) werden angehört und das Europäische Parlament kann sein Kontrollrecht ausüben.

Einer hat sich jedenfalls schon geäußert. Max Schrems kritisierte (nachzulesen unter www.noyb.eu/de/executive-order-zur-us-ueberwachung-reicht-wohl-nicht), dass die Executive Order die amerikanischen Überwachungsmaßnahmen nicht einschränken werden, dass das Data Protection Review Court (DPRC) kein wirkliches Gericht (sondern eher eine Art Ombudsstelle) ist und Betroffene weiterhin nicht informiert werden, ob sie tatsächlich von einer Überwachung betroffen waren. noyb analysiert aktuell die Rechtslage tiefergehend und wird dann entscheiden, ob es zu einer Entscheidung Schrems III kommen wird.

Teil 9:

Roadmap to Compliance

The Roadmap to Compliance

Sie brauchen ein Frühwarnsystem mit Beobachtungsturm und ein neues Risikoverständnis hinsichtlich 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

Die neue Compliance-Verantwortung

Datenschutz und Datensicherheit bei der Bearbeitung von Personendaten gehört in die Risikomatrix (IKS) einer Unternehmung oder Behörde.

Dieses neue strategische Risiko (Compliance-Verantwortung) muss

- jährlich einmal überprüft und schriftlich protokolliert werden
- allfällige Beurteilungen (Personendaten, besonders schützenswerte Personendaten, Profiling-Daten) aktualisiert werden sowie
- getroffene organisatorische und technische Massnahmen dem Stand der Technik und Bedrohungslage angepasst werden wie auch
- bestehende oder neue Datenbearbeitungsverhältnisse (ADVV-Anpassungen) überprüft werden
- Festgelegte Prozesse (Auskunft, Berichtigung, Löschung, Meldung, Benachrichtigung, Datenschutz-Vertreter etc.) kontrolliert und korrigiert werden

Die 7 wichtigsten Umsetzungsaktivitäten

Personendaten (1,2 und 3a/3b Personendaten, besonders schützenswerte Personendaten, Profiling-Daten und Profildaten mit hohem Risiko) evaluieren

Informationspflichten und Dokumentationspflichten erfüllen (Webseiten-Scan) **Bearbeitungsverzeichnis, Datenschutz-Folgeabschätzung, neue Datenschutzbestimmungen**

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

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

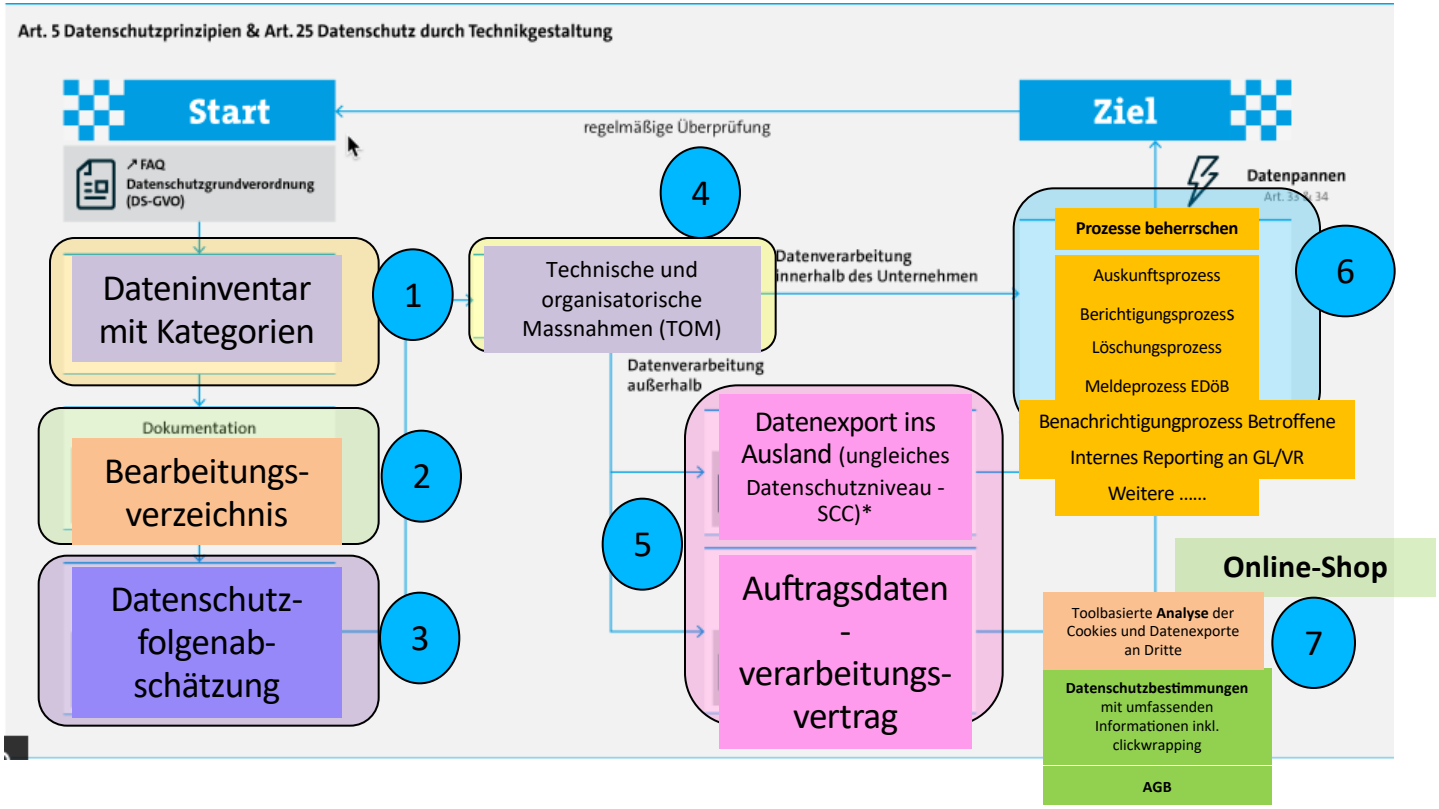
14. Online-Shops **umfassende Informationspflichten** bezüglich Einsatz von Cookies, Profiling-Tools, Targeting-Tools oder Einsatz weiterer Erfassungswerkzeuge prüfen und Datenschutzbestimmungen anpassen. — Muss-Anforderung

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

Umsetzungsmodell

FSDZ Rechtsanwälte & Notariat AG

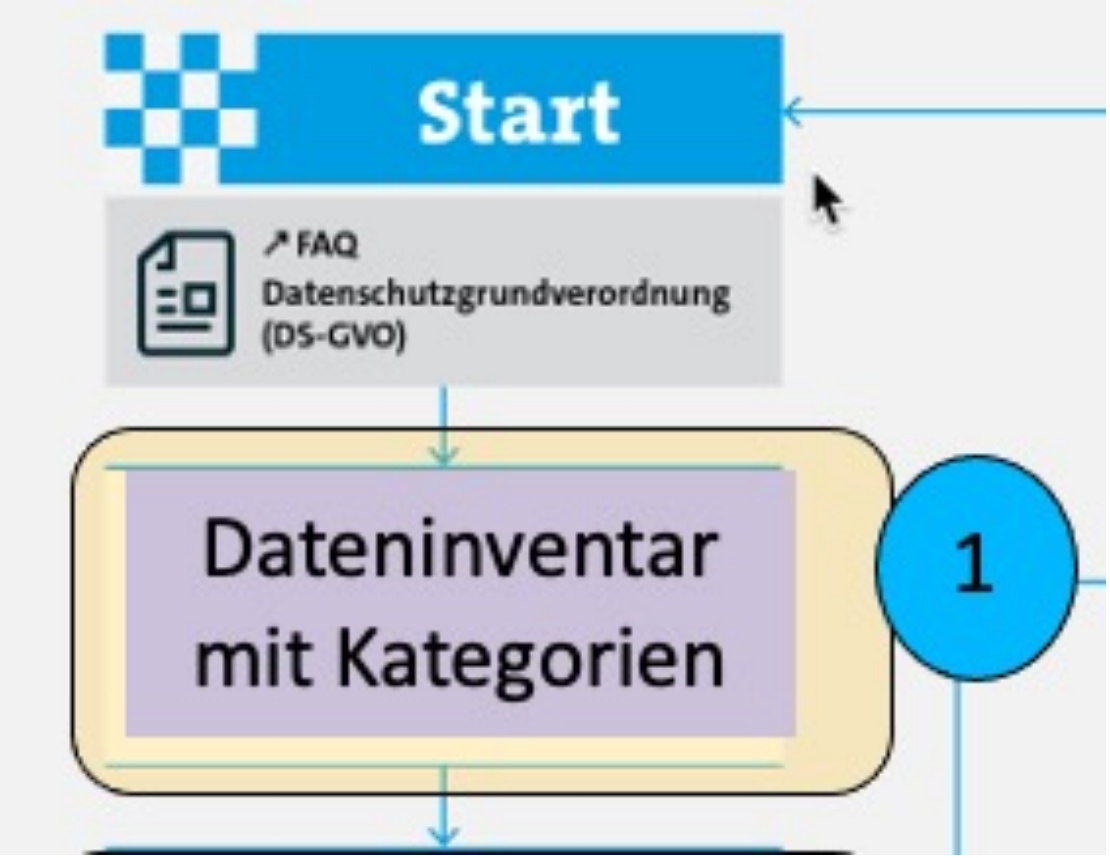
Umsetzung EU- und CH Datenschutz



Quelle: https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/Inhaltsseite-2.html
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom)

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

Dateninventar



Schritt 1a

Dateninventar der Unternehmung erstellen

a. Mitarbeiterdaten
b. Kundendaten
c. Lieferantendaten
d. Weitere Personendaten ….

Interne Bearbeitung

Externe Bearbeitung EU

Externe Bearbeitung andere Staaten

* Besonders schützenswerte Personendaten oder Profiling-Daten mit hohem Risiko

Mitarbeiter	Kunden	Lieferanten	Weitere Personendaten Behörden, Hilfspersonen, andere Dritte
Personalien *	Adressdaten *	Adressdaten *	Adressdaten
Bewerbungsdaten *	Bestelldaten *	Vertragsdaten	
Lohn- und Spesendaten	Finanzdaten	Bestelldaten	Finanzdaten
Sozialversicherungsdaten	Kommunikationsdaten	Finanzdaten	Kommunikationsdaten *
Gesundheitsdaten *	Supportdaten *	Kommunikationsdaten *	Supportdaten *
Administrativdaten *		Supportdaten *	
Aus- und Weiterbildungsdaten			
Mitarbeitergespräche			
.....	.....	.....	.....

Schritt 1b
Dateninventar der Unternehmung erstellen

Welche konkreten **Personendaten** pro Gruppe sammeln Sie?

z.B. Kundendaten (ordentliche Personendaten)

- Name
- Vorname
- Strasse
- Ort und PLZ
- Telefon
- E-Mail
- Verkaufsdaten (Medikamente, Bezugsdatum, Bezugsvolumen, Referenz auf Rezept ……. Etc.)
- Kreditkarten oder Bankdaten
- Rechnungsdaten
- ……

Hier anstatt Beschreibung allenfalls als Print-Sceens aus IT-Applikationen einbinden.

Schritt 1c
Dateninventar der Unternehmung erstellen

Welche konkreten Personendaten pro Gruppe sammeln Sie?

z.B. Kundendaten (besonders schützenswerte Personendaten)

- Blutgruppe
- Geschlecht
- Biometrische Information
- Rasse
- DNA-Sequenzinformation
- ……

Schritt 1d

Kategorien von Personendaten

Zuordnung der bearbeiteten Personendaten zu Kategorien

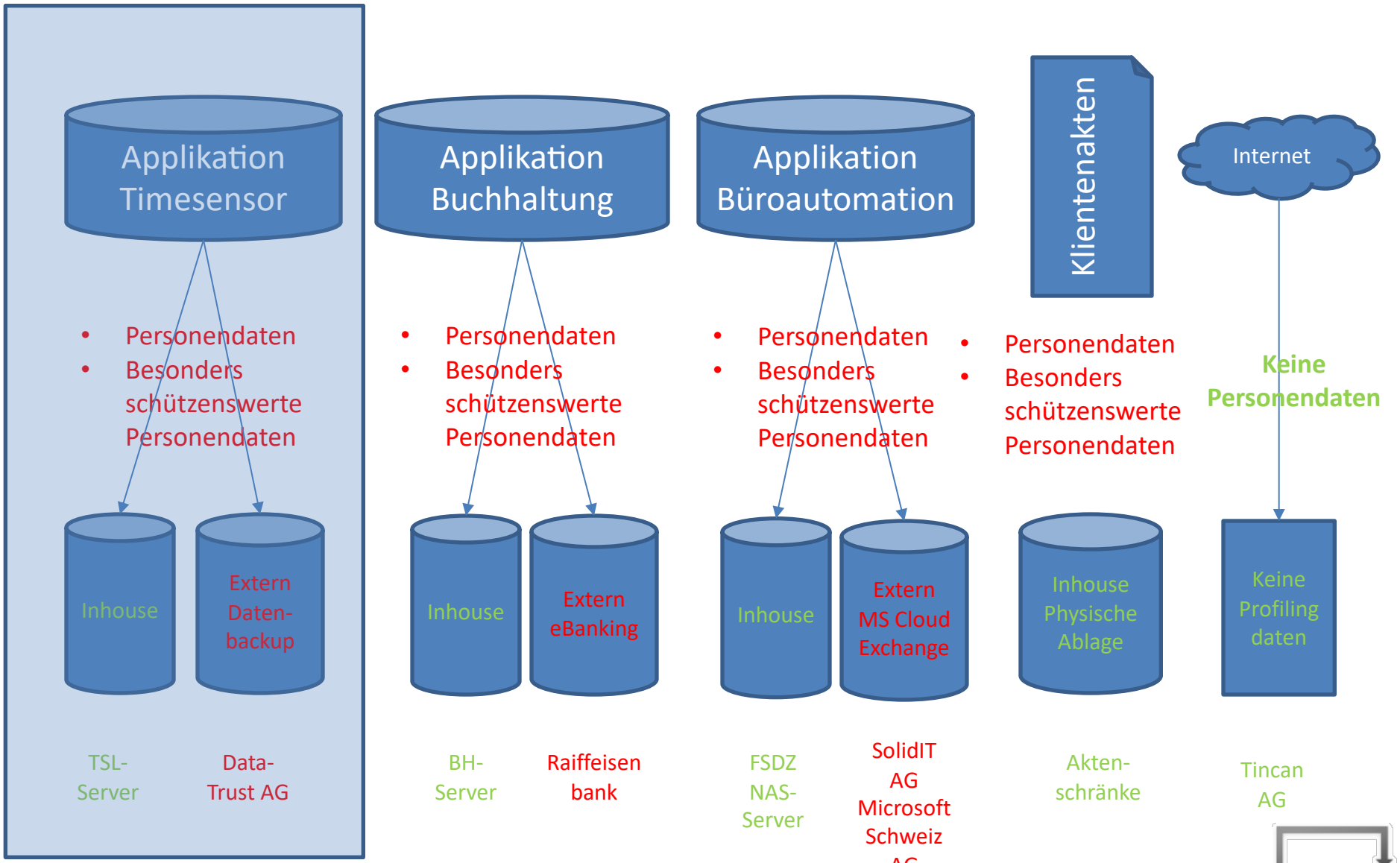
a. Personendaten
b. Besonders schützenswerte Personendaten
c. Profiling-Daten
    a. Ohne hohes Risiko für Rechte der Betroffenen
    b. Mit hohem Risiko für Rechte der Betroffenen (Folgenabschätzung)
d. Weitere Kategorien …..

Erste Checkliste mit Prüffragen zur Erstellung des Dateninventars

Vorlage Erstellung Personendaten Landkarte (Musterdokument)

	Frage / Ausgangslage	Fachabteilung (bspw. Logistik, HR etc.) Verantwortliche Person
1	Werden Personendaten bearbeitet? Falls ja: 1.1 - 1.3 ausfüllen.	
1.1	Werden besonders schützenswerte Daten berarbeitet? (z.B. Daten über die Gesundheit, Strafregisterauszüge)	
1.2	Werden Profiling-Daten gesammelt und/oder bearbeitet?	
1.3	Werden Profiling-Daten mit hohem Risiko gesammelt und/oder bearbeitet?	
2	Welche Bearbeitungstätigkeiten werden ausgeführt?	
3	Welche Applikationen werden benutzt? (vollständige Angabe) Wo sind diese Applikationen installiert? Intern oder extern?	
4	Wo werden die Daten gespeichert?	
5	Werden physischen Akten gesammelt und/oder bearbeitet? Wenn ja: Welche physischen Datensammlungen bestehen und zu welchem Zweck dienen sie?	
6	Gibt es externe Auftraggeber für die Datenbearbeitung?	
7	Wie werden die Daten vernichtet bzw. gelöscht und wie wird die Ausführung dokumentiert? Gibt es eine Prozessbeschreibung?	
8	Wer ist für die jeweiligen Bearbeitungstätigkeiten verantwortlich und zuständig?	

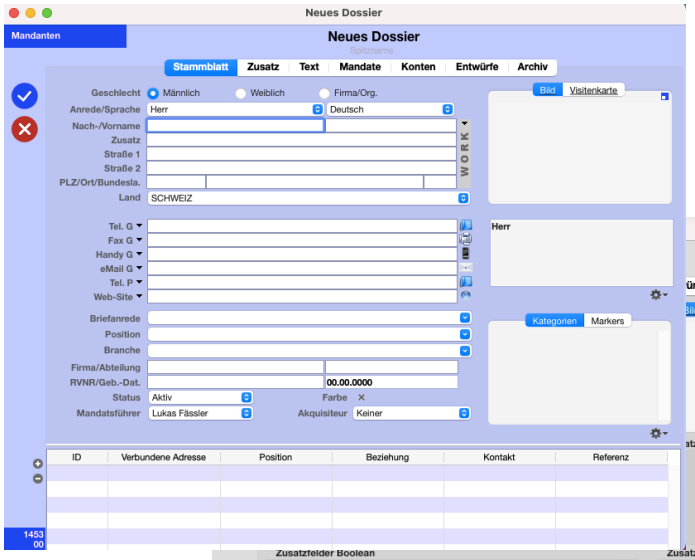
Inventar der Personendaten

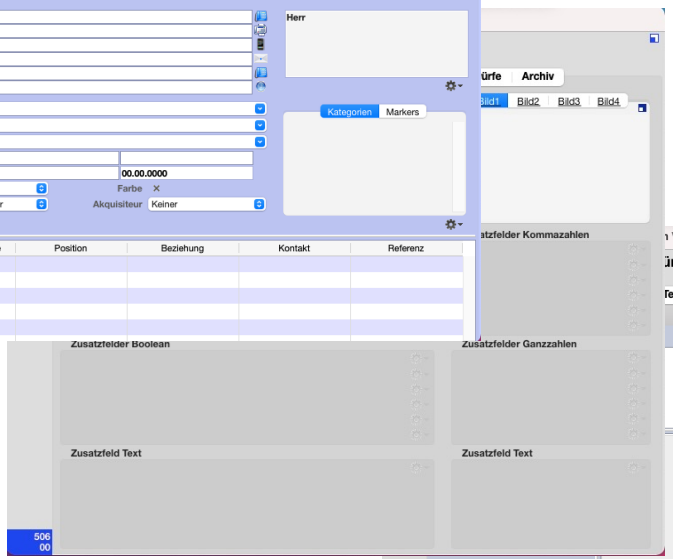


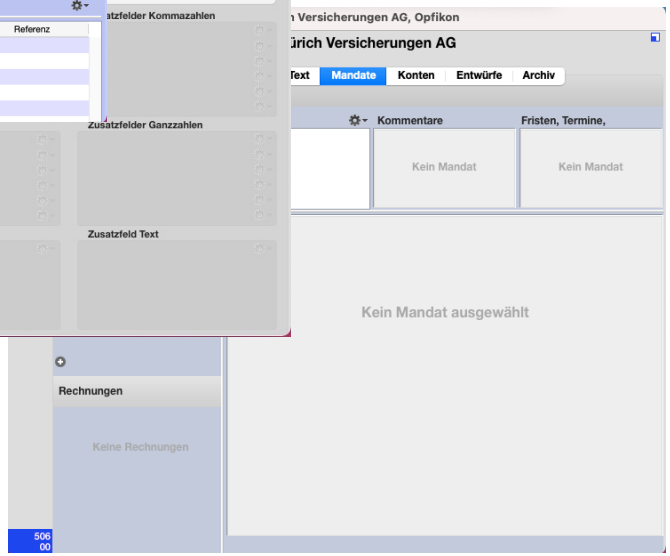
Inventar der Personendaten

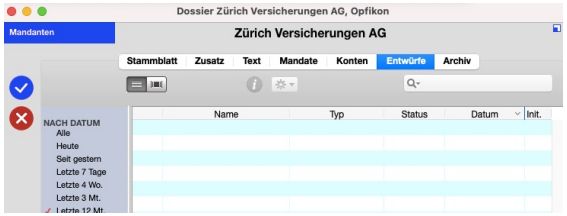
Applikation Timesensor

- Personendaten
- Besonders schützenswerte Personendaten









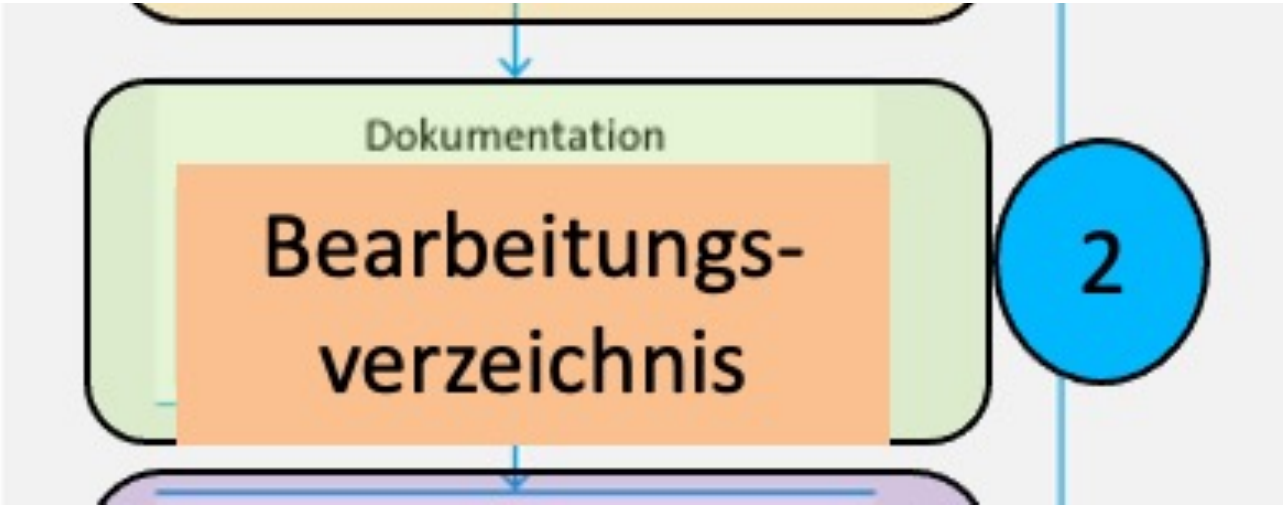
Inventar der Personendaten

Programm	Datenkategorien	Datenunterkategorien
Time Sensor Legal	Stammdaten	o Name o Geschlecht o Titel o Adresse o Telefonnummern (privat/geschäftlich/mobil) o E-Mail-Adresse o Webseite o Firma o Firmenadresse o Geschäftliche Position o Unspezifische Informationen zur Ergänzung
	Mandatsführungsdaten	o Bearbeitungsdaten o Stundenansätze o Aufwand in Stunden o Beschrieb der Leistungen
	Rechnungsdaten	o Kontendaten o Guthaben o Mahnungen
	Unstrukturierte Inhaltsdaten im Zusammenhang mit der Dossierbearbeitung im fallspezifischen Entwurfs- oder Archivbereich, u.a.:	o Finanzielle Situation (Betreibungen, Einkommen, Vermögen) o Nationalität o Gesundheit o Geburtsdatum o AHV-Nummer o Beruf und Ausbildung o Rassische und ethnische Herkunft o Politische Meinungen o Religiöse und weltanschauliche Überzeugungen o Gewerkschaftszugehörigkeit o Genetische und biometrische Daten o Sexuelle Orientierung o Massnahmen der sozialen Hilfe o Administrative und strafrechtliche Sanktionen und Verfolgung

Inventar der Personendaten

E-Mail-Exchange	Stammdaten der Korrespondenzpartner	o Name o E-Mail-Adresse
	Daten aus E-Mail-Header	
	Unstrukturierte Inhaltsdaten aus E-Mail-Body, ggf. Inhaltsdaten aus Anhängen	o Finanzielle Situation (Betreibungen, Einkommen, Vermögen) o Nationalität o Gesundheit o Geburtsdatum o AHV-Nummer o Beruf und Ausbildung o Rassische und ethnische Herkunft o Politische Meinungen o Religiöse und weltanschauliche Überzeugungen o Gewerkschaftszugehörigkeit o Genetische und biometrische Daten o Sexuelle Orientierung o Massnahmen der sozialen Hilfe o Administrative und strafrechtliche Sanktionen und Verfolgung
	Kalenderdaten	o Standortdaten o Termine o Gesprächsteilnehmer o Thematik<
Physische Hängeregistratur	Stammdaten	o Name o Geschlecht o Titel o Adresse o Telefonnummern (privat/geschäftlich/mobil) o E-Mail-Adresse o Webseite o Firma o Firmenadresse o Geschäftliche Position

Bearbeitungsverzeichnis



Schritt 2
Bearbeitungsverzeichnis

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.

Schritt 2
Bearbeitungsverzeichnis

Art. 5 Bearbeitungsreglement von privaten Personen

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

a. besonders schützenswerte Personendaten in grossem Umfang bearbeiten; oder

b. ein Profiling mit hohem Risiko durchführen.

2 Das Reglement muss insbesondere Angaben zur internen Organisation, zum Datenbearbeitungs- und Kontrollverfahren sowie zu den Massnahmen zur Gewährleistung der Datensicherheit enthalten.

3 Der private Verantwortliche und sein privater Auftragsbearbeiter müssen das Reglement regelmässig aktualisieren. Wurde eine Datenschutzberaterin oder ein Datenschutzberater ernannt, so muss dieser oder diesem das Reglement zur Verfügung gestellt werden.

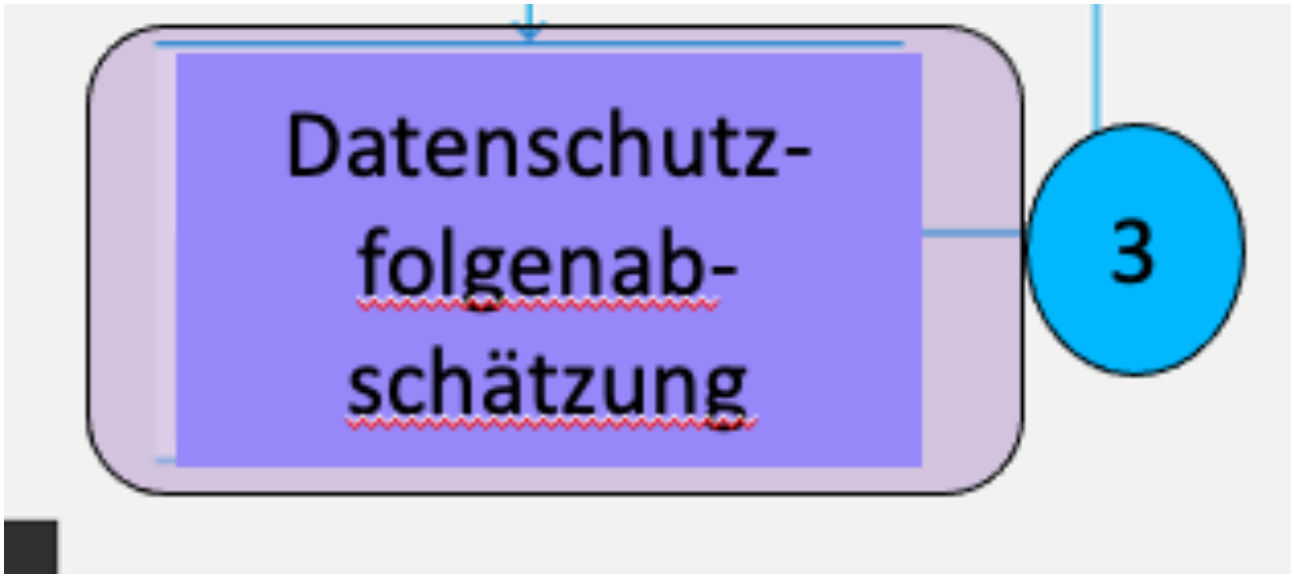
Schritt 2
Bearbeitungsverzeichnis

Verarbeitungstätigkeiten

Für die allgemeinen technischen und organisatorischen Massnahmen wird auf die TOM im Anhang verwiesen.
Gemeinsam für die Datenverarbeitung Verantwortliche liegen nicht vor; die alleinige Verantwortung liegt beim oben genannten Verantwortlichen.

	Zweck	Kategorien betroffener Personen	Kategorien personenbezogener Daten	Empfänger	Transfer an Drittstaat	Löschfrist	Techn. u. organis. Massnahmen	Datum der letzten Änderung
Betrieb der Mandantenverwaltungs-software Time Sensor Legal	Administrative Mandantenverwaltung; Juristische Dossierbearbeitung; Rechnungsstellung und Buchhaltung	Mandanten; ggf. Dritte (u.a. Gegenparteien, Behörden; Behörden; Banken)	Stammdaten Mandanten; Rechnungsdaten; Mandatsbearbeitungsdaten; Unstrukturierte Inhaltsdaten im Zusammenhang mit der Dossierbearbeitung im fallspezifischen Entwurfs- oder Archivbereich	Mitarbeitende; fineassist Treuhand; timeSensor AG	nein	10 Jahre nach Ablauf des Geschäftsjahres, in dem Schlussrechnung beglichen wurde (Aufbewahrungsfrist der Geschäftsbücher gemäss Art. 958f Abs. 1 OR)	Es wird auf die TOMs verwiesen.	29.05.2018
Betrieb des Netzwerkspeichers mydata	Administrative Mandantenverwaltung; Juristische Dossierbearbeitung; Rechnungsstellung und Buchhaltung	Mandanten; ggf. Dritte (u.a. Gegenparteien, Behörden; Behörden; Banken)	Stammdaten Mandanten; Rechnungsdaten; Mandatsbearbeitungsdaten; Unstrukturierte Inhaltsdaten im Zusammenhang mit der Dossierbearbeitung im fallspezifischen Ordner	Mitarbeitende	nein	10 Jahre nach Ablauf des Geschäftsjahres, in dem Schlussrechnung beglichen wurde (Aufbewahrungsfrist der Geschäftsbücher gemäss Art. 958f Abs. 1 OR)	Es wird auf die TOMs verwiesen.	29.05.2018
Betrieb einer Hängeregistratur	Administrative Mandantenverwaltung- Juristische Dossierbearbeitung	Mandanten; ggf. Dritte (u.a. Gegenparteien, Behörden; Behörden; Banken)	Stammdaten Mandanten; Rechnungsdaten; Unstrukturierte Inhaltsdaten im Zusammenhang mit der Dossierbearbeitung	Mitarbeitende	möglich	10 Jahre nach Ablauf des Geschäftsjahres, in dem Schlussrechnung beglichen wurde (Aufbewahrungsfrist der Geschäftsbücher gemäss Art. 958f Abs. 1 OR)	Klicken Sie hier, um Text einzugeben.	29.05.2018

Datenschutzfolgeabschätzung



Schritt 3
Datenschutz-Folgenabschätzung

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-Verordnung

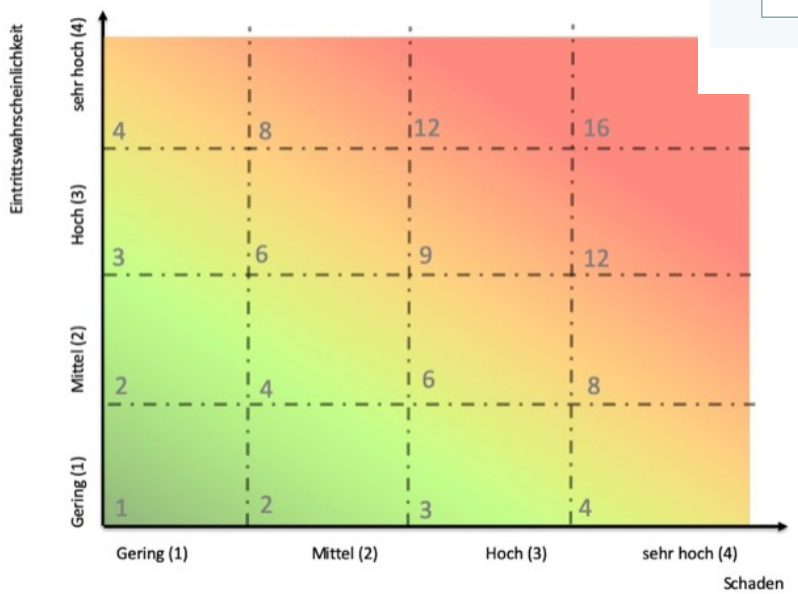
Art. 14 Aufbewahrung der Datenschutz-Folgenabschätzung

Der Verantwortliche muss die Datenschutz-Folgenabschätzung nach Beendigung der Datenbearbeitung mindestens zwei Jahren aufbewahren.

Datenschutz-Folgenabschätzung nach nDSG-CH

Beispiel

Risikomatrix



NORM [AKTUELL]

ISO/IEC 27005:2018-07

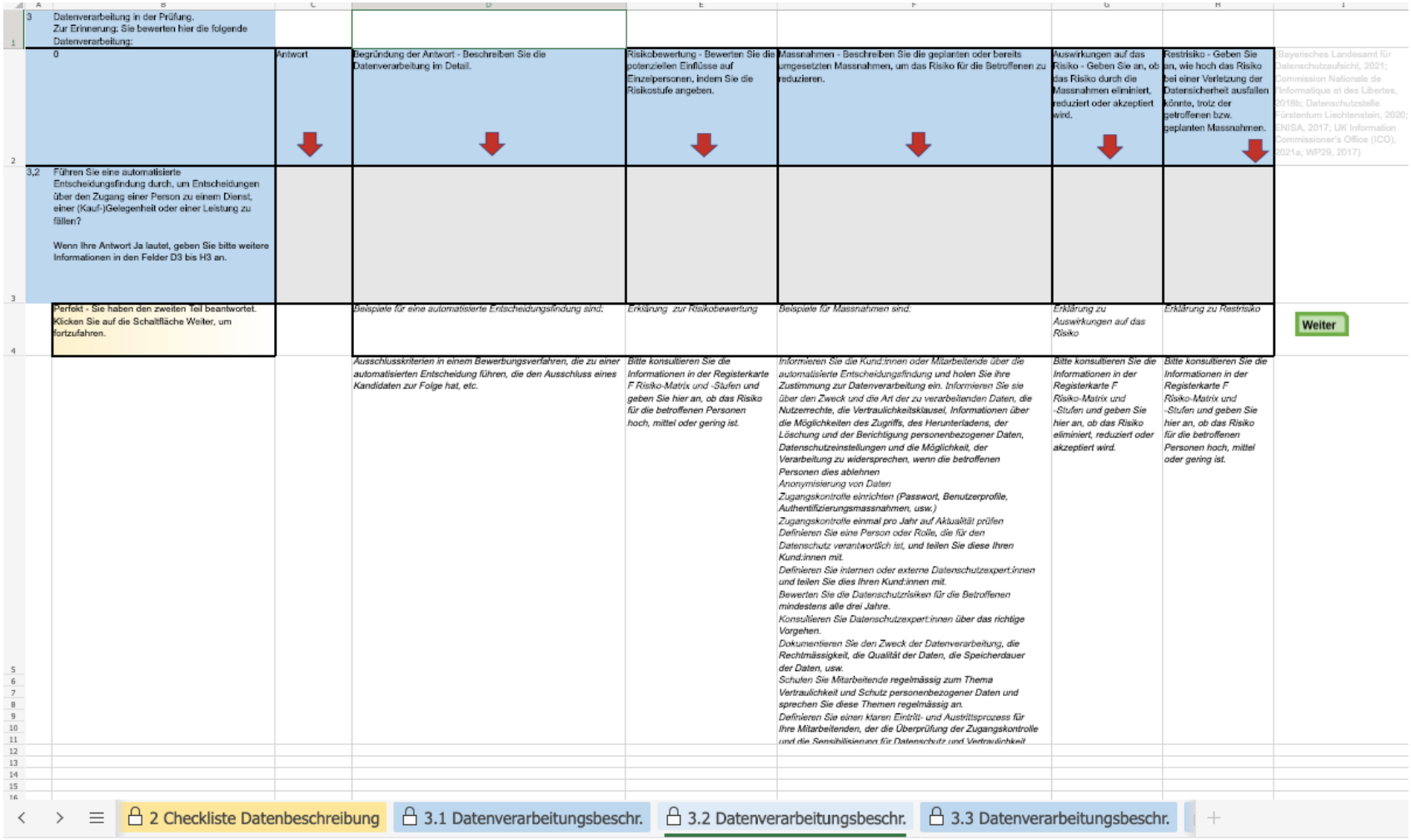
Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement

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

Ausgabedatum:
2018-07

Originalsprachen:
Englisch

Datenschutz-Folgenabschätzung nach nDSG-CH - Werkzeug



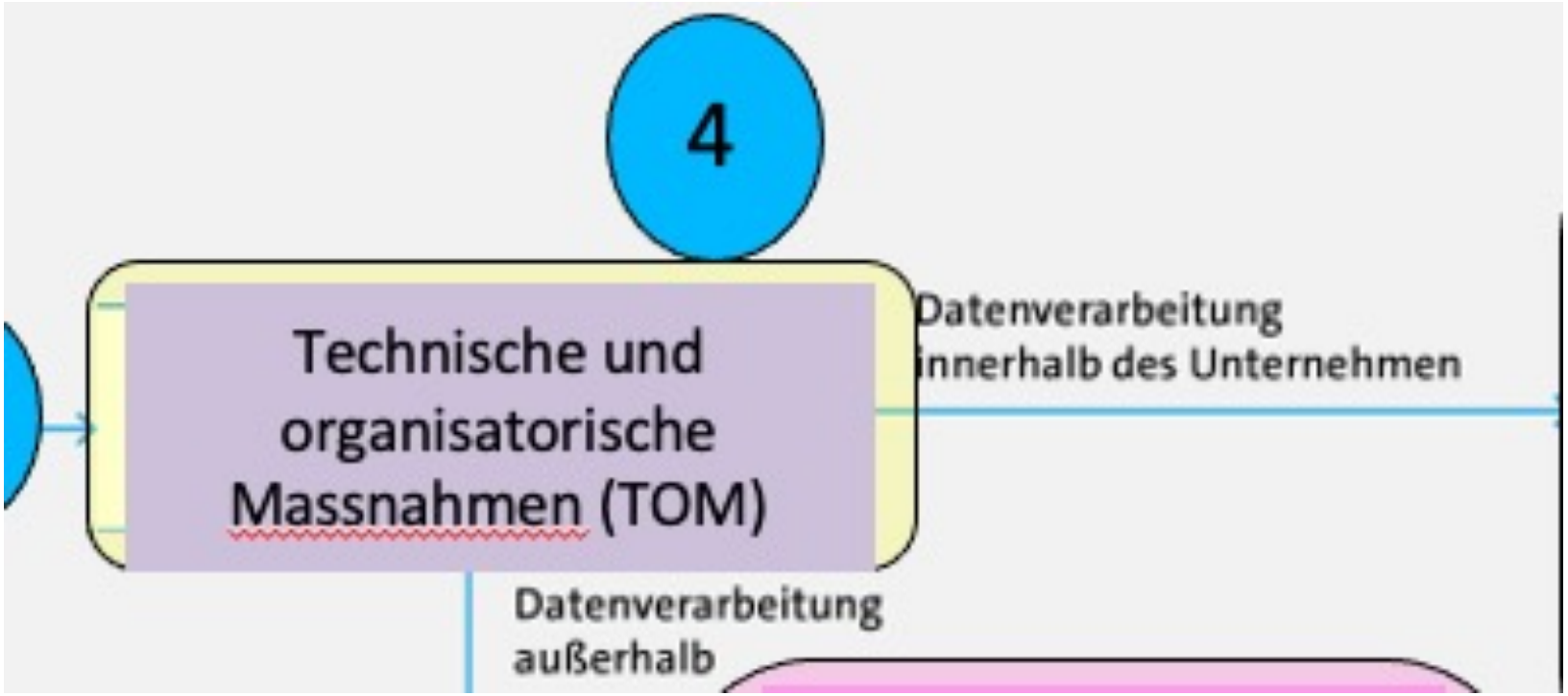
3	Datenverarbeitung in der Prüfung. Zur Erinnerung: Sie bewerten hier die folgende Datenverarbeitung:							
	0	Antwort	Begründung der Antwort - Beschreiben Sie die Datenverarbeitung im Detail.	Risikobewertung - Bewerten Sie die potenziellen Einflüsse auf Einzelpersonen, indem Sie die Risikostufe angeben.	Massnahmen - Beschreiben Sie die geplanten oder bereits umgesetzten Massnahmen, um das Risiko für die Betroffenen zu reduzieren.	Auswirkungen auf das Risiko - Geben Sie an, ob das Risiko durch die Massnahmen eliminiert, reduziert oder akzeptiert wird.	Restrisiko - Geben Sie an, wie hoch das Risiko bei einer Verletzung der Datensicherheit ausfallen könnte, trotz der getroffenen bzw. geplanten Massnahmen.	Bayerisches Landesamt für Datenschutzaufsicht, 2021; Commission Nationale de l'informatique et des Libertes, 2018b; Datenschutzstelle Fürstentum Liechtenstein, 2020; ENISA, 2017; UK Information Commissioner's Office (ICO), 2021a; WP29, 2017)
3,2	Führen Sie eine automatisierte Entscheidungsfindung durch, um Entscheidungen über den Zugang einer Person zu einem Dienst, einer (Kauf-)Gelegenheit oder einer Leistung zu fällen? Wenn Ihre Antwort Ja lautet, geben Sie bitte weitere Informationen in den Felder D3 bis H3 an.							
	Perfekt - Sie haben den zweiten Teil beantwortet. Klicken Sie auf die Schaltfläche Weiter, um fortzufahren.		*Beispiele für eine automatisierte Entscheidungsfindung sind:* *Ausschlusskriterien in einem Bewerbungsverfahren, die zu einer automatisierten Entscheidung führen, die den Ausschluss eines Kandidaten zur Folge hat, etc.*	*Erklärung zur Risikobewertung* *Bitte konsultieren Sie die Informationen in der Registerkarte F Risiko-Matrix und -Stufen und geben Sie hier an, ob das Risiko für die betroffenen Personen hoch, mittel oder gering ist.*	*Beispiele für Massnahmen sind:* *Informieren Sie die Kund:innen oder Mitarbeitende über die automatisierte Entscheidungsfindung und holen Sie ihre Zustimmung zur Datenverarbeitung ein. Informieren Sie sie über den Zweck und die Art der zu verarbeitenden Daten, die Nutzerrechte, die Vertraulichkeitsklausel, Informationen über die Möglichkeiten des Zugriffs, des Herunterladens, der Löschung und der Berichtigung personenbezogener Daten, Datenschutzeinstellungen und die Möglichkeit, der Verarbeitung zu widersprechen, wenn die betroffenen Personen dies ablehnen* *Anonymisierung von Daten* *Zugangskontrolle einrichten (Passwort, Benutzerprofile, Authentifizierungsmassnahmen, usw.)* *Zugangskontrolle einmal pro Jahr auf Aktualität prüfen* *Definieren Sie eine Person oder Rolle, die für den Datenschutz verantwortlich ist, und teilen Sie diese Ihren Kund:innen mit.* *Definieren Sie internen oder externe Datenschutzexpert:innen und teilen Sie dies Ihren Kund:innen mit.* *Bewerten Sie die Datenschutzrisiken für die Betroffenen mindestens alle drei Jahre.* *Konsultieren Sie Datenschutzexpert:innen über das richtige Vorgehen.* *Dokumentieren Sie den Zweck der Datenverarbeitung, die Rechtmässigkeit, die Qualität der Daten, die Speicherdauer der Daten, usw.* *Schulen Sie Mitarbeitende regelmässig zum Thema Vertraulichkeit und Schutz personenbezogener Daten und sprechen Sie diese Themen regelmässig an.* *Definieren Sie einen klaren Eintritt- und Austrittsprozess für Ihre Mitarbeitenden, der die Überprüfung der Zugangskontrolle und die Sensibilisierung für Datenschutz und Vertraulichkeit*	*Erklärung zu Auswirkungen auf das Risiko* *Bitte konsultieren Sie die Informationen in der Registerkarte F Risiko-Matrix und -Stufen und geben Sie hier an, ob das Risiko eliminiert, reduziert oder akzeptiert wird.*	*Erklärung zu Restrisiko* *Bitte konsultieren Sie die Informationen in der Registerkarte F Risiko-Matrix und -Stufen und geben Sie hier an, ob das Risiko für die betroffenen Personen hoch, mittel oder gering ist.*	Weiter

2 Checkliste Datenbeschreibung | 3.1 Datenverarbeitungsbeschr. | 3.2 Datenverarbeitungsbeschr. | 3.3 Datenverarbeitungsbeschr.

Technische & organisatorische Massnahmen

Schritt 4

Technische & organisatorische Massnahmen pro Personendatensatz / Personendatenkategorien festlegen



Xplain-Fall
Schlussbericht des EDÖB

Schlussbericht und Empfehlungen

vom 25. April 2024

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)

in Sachen Xplain AG

aufgrund Ransomware-Vorfall

gemäss

Artikel 29 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (aDSG) in Verbindung mit Artikel 70 Bundesgesetz vom 25. September 2020 über den Datenschutz (DSG)

Ausgangslage

- EDÖB hat eine Sachverhaltsabklärung gegenüber Xplain gestützt auf **Art. 29 aDSG** am 13.7.2023 eröffnet. Inkrafttreten neues DSG am 1.9.2023.

- Neben originären Daten von Xplain (Angaben über Kunden oder Mitarbeitende) waren auch eine hohe Anzahl von Personendaten aus der Bundesverwaltung, die strafrechtliche Verfolgungen und Sanktionen betreffen und per se als besonders schützenswerte Personendaten (Art. 3 lit. c Ziffer 4 sDSG) betroffen.
- DIese Daten waren auf einem Fileserver von Xplain gespeichert.
- Hackergruppe PLAY hat sich im Mai 2023 Zugang zu einem von der FIRMA XY AG gehosteten Server von Xplain verschafft und sich mittels „lateral Movement“ durch das Netzwerk der Xplain vorgearbetet. Schliesslich landete die Hackergruppe auf dem Fileserver von Xplain am Standort in Interlaken.

- Verträge basieren auf Vorlagen BIT und AGB Bund (Ausgabe 2010) für alle Vertragstypen. Ziffer 8 AGB Dienstleistungen; Ziffer 22 und 23 AGB Werkvertrag; Ziffer 24 und 25 AGB Pflege

IT-Infrastrukturen Xplain - Findings

- Fileserver verfügt nicht über aktuellen Patchlevel Rz 10
- Unnötig geöffnete Ports aufweisend Rz 10
- Auf Server lief kein aktives Monitoring, welches ungewöhnliche Aktivitäten oder Anomalien zeitnah erkannt werden konnten Rz 10
- Es habe gemäss Xplain dazu keine vertragliche Verpflichtung zur Datenbearbeitung gegeben Rz 10
- Monatliche Loganalysen seien implementiert gewesen Rz 10
- Patch-Management-Prozess für Systeme und Software sei implementiert gewesen Rz 10
- Xplain verfügte über kein SOC, da vertraglich dazu nicht verpflichtet Rz 11
- Xplain habe über ausgewiesenes und ausgebildetes IT-Security-Fachpersonal verfügt RZ 11

IT-Infrastrukturen Xplain – Findings (2)

- Über organisatorische und technische Massnahmen der Datensicherheit lagen keine Dokumente vor. Sie seien beim Ransomware-Angriff gelöscht worden (?) Rz 12
- Xplain war nach ISO9001 zertifiziert. Nicht nach ISO27001 zertifiziert Rz 12
- Xplain verfügte offenbar über keine VR-Vorgaben bezüglich Beachtung von Standards für die Informations-Sicherheit

- Xplain hatte eine Cyberversicherung abgeschlossen, welche Obliegenheiten für Xplain definiert hatte: Rz 13
  - regelmässige Backups
  - Internetschutzprogramme
  - Antivirussoftware
  - Firewall
  - Zeitnahes Patching der Systeme

IT-Infrastrukturen Xplain – Findings (3)

- 1.5 TB Daten auf betroffenem Server gespeichert. Davon wurden 907 GB Daten im Darknet publiziert. 424 GB Daten gemäss Analyse NCSC relevante Daten 5182 Objekte mit sensitivem Inhalt Rz 16
- Daten sind von den Kunden (FedPol, BAZG) unverschlüsselt an Xplain übermittelt worden. Rz 17
- Unterscheidung zwischen relevanten und nicht relevanten Daten Rz 18
  Relevante Daten sind Inhalte wie Personendaten, technische Informationen, Klassifizierte Informationen und Passwörter

- Offenbar wurden Supportfalldaten aus dem Jahre 2014/2015 auf dem persönlichen Laufwerk eines Leadentwicklers gespeichert und entwendet Rz 21

IT-Infrastrukturen Xplain – Findings (4)

- Datenübertragung von Kunden (FedPol, BAZG) wurden aufgrund von Fehleranalysen der Applikationsverantwortlichen nachgebildet, kommentiert und an Xplain übermittelt. Dort wurden diese Daten entweder auf zugriffsgeschützten Laufwerken oder auf dedizierten Geräten analysiert. Rz 24

- Fehlerberichte und dazugehörige Personendaten werden auf einem Fileshare für Xplain zur Abholung (Remotezugriff) bereitgestellt. Rz 31

- Eine direkte Uebermittlung von Fehlermeldungen an einen externen FTP-Server von Xplain war im Netz der BV unterbunden Rz 32

- Xplain-Mitarbeiter haben keinen Zugriff auf die im ISC-EJPD betriebenen Applikationen. Rz 36

- Mitarbeiter von Xplain, welche direkt mit BV zusammenarbeiteten, wurden einer internen Personensicherheitsüberprüfung unterzogen

IT-Infrastrukturen Xplain – Findings (5)

- Eine möglichst konkrete REGELUNG DER DATENÜBERTRAGUNG AN DRITTE in Supportfällen ist zum Vorteil des Verantwortlichen, da er gegenüber den betroffenen Personen die datenschutzrechtliche Verantwortung trägt. Rz 110

- Die Support- und Wartungsprozezsse sind vertraglich nur rudimentär geregelt worden. Rz 111

- Eine **verschlüsselte** Uebermittlung von Personendaten wurde vertraglich nicht festgelegt. Rz 111

- Xplain hat die ihr übergebenen Personendaten so zu bearbeiten, wie es nach den vertraglichen Vorgaben vorgegeben ist und was der Auftraggeber selber tun dürfte (Art. 10a Abs. 1 lit. a aDSG) Rz 118

- Weitere Vorgaben finden sich in Art. 8 und 9 aDSG Rz 122

IT-Infrastrukturen Xplain – Findings (6)

- Dokumentationen zur Datensicherheit und den Aufgaben und Prozessen der Datensicherheit und der dafür zuständigen Personen beim Auftragsdatenverarbeiter müssen auch nach gravierenden IT-Störungen greifbar sein (physisch aufzubewahren). Rz 126

- Verlangt wird eine Sicherheitsinfrastruktur, welche die Integrität der Software in Bezug auf das Bearbeiten von besonders schützenswerten Personendaten gewährleisten kann (Art 13 und 7 nDSG). Rz 128

- Der Software-Entwicklungsprozess (mit Wartung, Pflege und Support) ist ein datenschutzrelevanter Prozess, der entsprechende Massnahmen der Datensicherheit verlangt. Rz 129

IT-Infrastrukturen Xplain – Findings (7)

- Xplain verfügte über kein Security Operation Center (SOC) und auf dem betroffenen Server lief kein aktives Monitoring. Rz 130
- Patches der Server erfolgten nur monatlich, sodass beim Angriff nicht die neuesten verfügbaren Patches eingespielt waren. Rz 130
- Die Umsetzung der getroffenen Massnahmen müssen von Xplain kontrolliert werden und diese Kontrollen müssen nachgewiesen werden. Rz 130
- Xplain verfügt nicht über eine Zertifizierung im Bereich ISO27001, die sicherstellt, dass bestimmte Standards in Bezug auf die Informationssicherheit eingehalten werden und Prozesse dazu (im ISMS) definiert sind. Rz 131
- Es liegen auch keine internen Auditberichte vor. Rz 132
- Vertragliche Verpflichtungen wurden auch nicht in die eigenen Prozesse bei Xplain übernommen Rz 132
- Es war eine Meldepflicht von 24 Stunden vertraglich vereinbart, die nicht eingehalten worden ist. Rz 153

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

5. Empfehlungen

158. Gestützt auf Art. 29 Abs. 3 aDSG erlässt der EDÖB gegenüber Xplain die folgenden Empfehlungen:

159. In Bezug auf die Verletzung des Grundsatzes der Datensicherheit (vgl. Kap. 4.6):

Empfehlungen:

Xplain trifft technische und organisatorische Massnahmen der Datensicherheit gemäss Art. 7 DSG (neu: Art. 8 DSG) und nach den Vorgaben der Bundesverwaltung (siehe Ziffer 70 ff.), die angemessen sind in Bezug auf

1. das Bearbeiten von besonders schützenswerten Personendaten im Rahmen von Support- und Wartungsprozessen, die Xplain als Dienstleiter anbietet,
2. das Bearbeiten von Personendaten unter einem qualifizierten Geheimnisschutz,
3. auf die Entwicklung von Software im sensitiven Bereich der Inneren Sicherheit.

Xplain hat die Einhaltung der technischen und organisatorischen Massnahmen gegenüber der Bundesverwaltung regelmässig nachzuweisen, indem

4. ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut wird,
5. ein Risikomanagement etabliert wird und eine laufende Evaluierung der Massnahmen stattfindet,
6. eine kontinuierliche Sensibilisierung der Mitarbeitenden erfolgt,
7. periodisch interne und externe Audits durchgeführt werden.

Solange Xplain im Bereich der Inneren Sicherheit mit der Bundesverwaltung zusammenarbeitet, ist

8. die Zertifizierung des ISMS nach einem international anerkannten Standard nachzuweisen.

160. In Bezug auf die Verletzung der Grundsätze der Rechtmässigkeit, der Verhältnismässigkeit und der Zweckbindung (vgl. Kap. 4.7)

Empfehlungen:

Xplain kommt seinen vertraglichen Pflichten als Auftragsbearbeiter gemäss Art. 10a aDSG (neu Art. 9 DSG) nach, indem

9. die Verpflichtungen aus den Verträgen mit der Bundesverwaltung in die eigenen technischen und organisatorischen Prozesse eingebunden werden,
10. ein Löschkonzept gemäss den gesetzlichen und vertraglichen Vorgaben umgesetzt wird.

Rechtsmittelbelehrung:

- Xplain hat 30 Tage Zeit zu erklären, ob sie die Empfehlungen des EDÖB akzeptiert und umsetzt.
- Lehnt sie ab, kann der EDÖB eine Verfügung erlassen, die dann ans Bundesverwaltungsgericht weitergezogen werden könnte.

Kanton Waadt kündigt Xplain-Vertrag

Von Reto Vogt, 8. Februar 2024, 17:24

POLITIK & WIRTSCHAFT BESCHAFFUNG KANTON WAADT XPLAIN

Foto: zVg

Xplain wurde von der Waadtländer Polizei mit der Modernisierung des IT-Systems beauftragt. Daraus wird nichts mehr. Xplain will prüfen, ob die Kündigung rechtens ist.

Am 7. Februar beschloss der Waadtländer Staatsrat, den Vertrag mit Xplain mit sofortiger Wirkung zu kündigen, um die "finanziellen und betrieblichen Risiken einzugrenzen", wie der Kanton in einer Mitteilung schreibt.

Durch den Cyberangriff auf Xplain wurde die Durchführung von Odyssée "erheblich gestört", was zu Verzögerungen geführt habe, wie es in der Mitteilung des Kantons weiter heisst. Bekannt ist das schon seit Herbst 2023, schon damals äusserten Mitglieder des Kantonsparlaments Bedenken.

Der Lieferant habe ausserdem "Probleme mit der Produktqualität", was zu "ernsthaften Zweifeln an seiner Fähigkeit führte, die ursprünglich vereinbarten Leistungen zu erbringen", schreibt der Kanton in ungewohnter Schärfe. Der Kanton arbeitet mit dem aktuellen System weiter, bis ein neuer Lieferant feststeht. Es bleibe aber eine Modernisierung erforderlich.

Reputationsschaden als schwerwiegendste Unternehmensproblematik

Xplain ist verkauft

Von Katharina Jochum, 17. Oktober 2024 um 09:50

CHANNEL XPLAIN CHAPTERS GROUP ÜBERNAHME VERWALTUNG

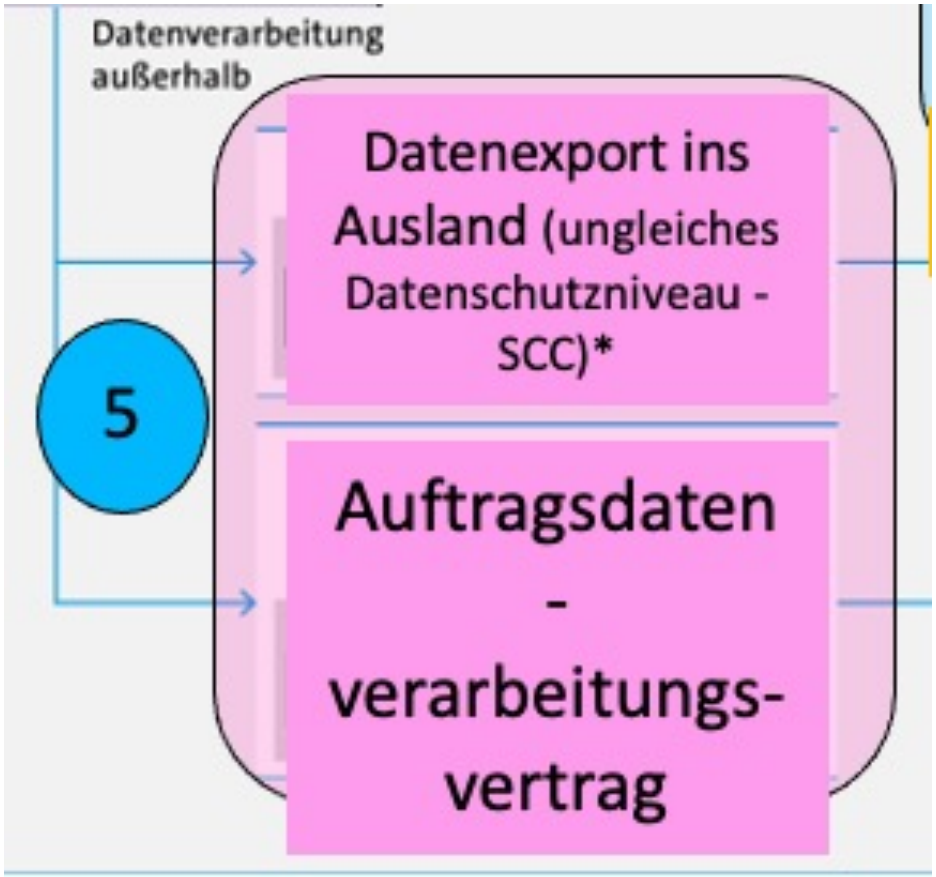
Das Büro von Xplain in Interlaken. Foto: Jag9889 / Wikimedia / Lizenz: CC BY-SA 4.0 Deed (zugeschnitten)

Die deutsche Chapters Group übernimmt sämtliche Anteile der Schweizer Softwarefirma. Nach dem schwerwiegenden Cyberangriff könne man jetzt "ein neues Kapitel aufschlagen".

Auftragsdatenverarbeitungsvertrag ADVV

Schritt 5

Auftragsdatenbearbeitungsvertrag ADV



Feedback-Version Verein 2.0 des Vereins SSGI vom 22.8.2024

hat gelöscht: Korrektur-

RAHMENVEREINBARUNG ÜBER DIE AUFTRAGS-DATENVERARBEITUNG

zwischen

Axians Infoma Schweiz AG
Suurstoffi 22
6343 Rotkreuz
als «Auftragsbearbeiterin»

und

Verein Schweizerische Städte- und Gemeinde-Informatik (SSGI)
Zugerstrasse 76B, CH-6340 Baar

INHALTSVERZEICHNIS

Anlage 1 – Angaben zur Bearbeitung von Personendaten

Zweck der Bearbeitung	Bearbeitung von Personendaten für den Verantwortlichen gemäss Vertrag zwischen den Parteien
Dauer der Bearbeitung	Während der Vertragsdauer resp. gemäss den gesetzlichen Vorgaben, soweit nicht explizit anders geregelt.
Kategorien von betroffenen Personen*	Kunden, Mitarbeiter, Lieferanten und Hersteller, potenzielle Kunden, Versicherte
Kategorien von personenbezogenen Daten*	Personalien und (End)Kundendaten (Name, Vorname, Adresse Geburtstag/Alter, E-Mail, Telefonnummer etc.) Bankdaten, Einwohner-/Endkundendaten (Nationalität, Kontonummer, Geschäftskorrespondenz, Falldaten wie Verfügungen oder Pfändungen, Systemdaten) Besonders schützenswerte Personendaten (Gesundheitsdaten, soweit vom Kunden bearbeitet, Religion, biometrische Daten für allfällige Zugangskontrolle, Sozialversicherungsdaten) Technische Daten wie IP-Adresse, Logfiles etc.
Ort der Lagerung und Bearbeitung	An der Geschäftsadresse der Auftragsbearbeiterin und seiner zugelassenen Unterauftragsbearbeiter gemäss Anlage 1
Review und Audit (virtuell oder ausnahmsweise vor Ort)	Ja (2 (zwei) Arbeitstage pro Jahr)
Spezifische Anweisungen oder andere Sonderbestimmungen	Anlage 2 – Technische und Organisatorische Massnahmen (TOM)
Überweisung ausserhalb der Schweiz und einem Land mit adäquatem Datenschutzniveau	Axians Infoma GmbH (Deutschland), Axians Infoma Romania SRL Im Übrigen mit vorgängiger Zustimmung gemäss diesem Anhang erlaubt

* Kategorien der Personendaten sowie der betroffenen Personen werden durch den Verantwortlichen und ohne Zutun der Auftragsbearbeiterin festgelegt. Die Aufzählung ist exemplarisch.

Anlage 2 – Technische und Organisatorische Massnahmen (TOM)

Diese Anlage beschreibt die technischen und organisatorischen Massnahmen (TOM), die die Auftragsbearbeiterin ergreift, um die Sicherheit der ihr anvertrauten personenbezogenen Daten des Kunden zu gewährleisten.

Zusätzliche Informationen über diese Massnahmen sind gemäss dem in der Rahmenvereinbarung vorgesehenen Auskunftsrecht zur Verfügung zu stellen.

1. Organisatorische Sicherheitsmassnahmen

1.1. Management von Sicherheitsmassnahmen

Sicherheitskonzept und -verfahren

Die Auftragsbearbeiterin verfügt über ein dokumentiertes Sicherheitskonzept für die Bearbeitung von personenbezogenen Daten. Dazu gehört insbesondere auch die Bearbeitung im Rahmen von Support- und Wartungsprozessen sowie Datenmigrationen.

Die in Anlage 2 definierten Tätigkeiten und Verhaltensweisen finden umfassenden Eingang in die Prozessdefinitionen der Auftragsbearbeiterin, werden verantwortlichen Prozesseignern zugewiesen und unterliegen einer mindestens einmal jährlich durchzuführenden, dokumentierten internen Überprüfung. Diese Auflage kann im Rahmen eines anerkannten internationalen Qualitätsmanagement-Systems sichergestellt werden.

Rollen und Verantwortlichkeiten

- Die Rollen und Verantwortlichkeiten bei der Auftragsbearbeiterin im Zusammenhang mit der Bearbeitung von Personendaten sind klar definiert und im Einklang mit dem Sicherheitskonzept zugewiesen.
- Bei internen Umstrukturierungen oder Kündigungen und beim Wechsel des Arbeitsplatzes ist

KI und Datenschutz

Appenzell Ausserrhoden

Merkblatt zur Verwendung von generativen KI-Werkzeugen in der KVAR (Stand: 29. Oktober 2024)

Was versteht man unter generativen KI-Werkzeugen?
Terminologie - CNAI - Kompetenznetzwerk für künstliche Intelligenz (z.B. ChatGPT, Bard, deepL)

Was ist im Hinblick auf die Nutzung von KI im geschäftlichen Bereich erlaubt?
Verantwortungsvolles Experimentieren ist erlaubt: Generative KI-Werkzeuge können Sie bei Ihrer täglichen Verwaltungstätigkeit unterstützen.

Was ist untersagt?
Es bleibt untersagt, bestehende Vorgaben zu verletzen. Dies bedeutet im Hinblick auf den Datenschutz und das Amtsgeheimnis analog der bisherigen Nutzung anderer Webapplikationen im Internet u.a.:

- Keine Eingabe von internen oder vertraulichen Informationen;
- Keine Eingabe von durch Datenschutz oder Amts- bzw. Berufsgeheimnis geschützte Daten;
- Keine Eingabe von Personendaten jeglicher Art. Auch bei der Eingabe von anonymisierten oder pseudonymisierten Eingaben besteht aktuell und umso mehr in Zukunft ein Restrisiko (vgl. z.B. KI gefährdet Anonymisierung von Gerichtsurteilen).

Wichtig: Bitte verzichten Sie im Zweifelsfall auf den Einsatz von generativen KI-Werkzeugen.

Beispiele Einsatz von generativen Werkzeugen

Generatives KI-Werkzeug erlaubt	Generatives KI-Werkzeug untersagt
Veröffentlichte Texte (z.B. Berichte) zusammenfassen lassen	Dokumente des Mitberichtsverfahrens zusammenfassen lassen (nicht öffentliche Dokumente)
Als Einstieg oder Einleitung für ein Thema (analog Google/Wikipedia)	Eingabe von urheberrechtlich geschützten Daten (Urheberrechtsverletzung)
Unterstützung beim Formulieren von Foliensätzen, Antworten auf Anfragen oder anderen Texten	Konkrete Anfrage von Hans Muster unverändert eingeben (Personendaten)
Bilder für Präsentationen erstellen lassen	KI-generierte Antworten copy/paste-artig verwenden (Kontrolle)

Wie sollen Ergebnisse verwendet werden? Was soll dabei beachtet werden?

- Generative KI-Werkzeuge liefern Ergebnisse unterschiedlicher Qualität.
- Überprüfen Sie die KI-Ergebnisse immer kritisch auf Richtigkeit und Vollständigkeit und vergleichen Sie diese mit anderen Quellen. Übernehmen Sie die KI-Ergebnisse nie unbesehen in Ihre Arbeit.
- Sie müssen Entscheidungen, welche auf Ergebnissen von generativen KI-Werkzeugen beruhen, jederzeit begründen können.
- Weisen Sie transparent auf die Nutzung von KI-Werkzeugen hin.
- Allenfalls beinhalten die Nutzungshinweise der gewählten generativen KI Hinweise auf die Weiterverwendung von Inhalten (Urheberrechte).
- Oftmals ist unklar, woher die KI-Ergebnisse stammen. Wer urheberrechtsverletzende Ergebnisse verwendet, begeht eine Urheberrechtsverletzung.

Wichtig: Die Verantwortung für das verwendete Ergebnis bleibt bei Ihnen, sie kann nicht an die KI delegiert werden.

Was soll bezüglich Sicherheit beachtet werden?
Gewisse Anwendungen sind aufgrund von Sicherheitsanforderungen innerhalb der Kantonsverwaltung gesperrt. Halten Sie die Bestimmungen zur Informatik- und Cybersicherheit jederzeit ein.

An wen kann ich mich innerhalb der KVAR mit Anliegen und Fragen rund um KI wenden?
Christian Bernhardsgrütter, Leiter Kanzleidienste (c.bernhardsgruetter@ar.ch), nimmt Anliegen und Fragen entgegen.

Quelle und weiterführende Informationen: Merkblatt Verwendung generativer KI-Werkzeugen in Bundesverwaltung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

18. Januar 2024 V1.2[1]

Merkblatt zur Verwendung von generativen KI-Werkzeugen in der Bundesverwaltung

Aktenzeichen: 822.1-1/8/5/1

Was sind generative KI-Werkzeuge?

Im Internet verfügbare Werkzeuge mit generativer künstlicher Intelligenz (KI)[2] – zum Beispiel ChatGPT von OpenAI, Copilot von Microsoft, Bard von Google, Grok von X und zahlreiche mehr – vereinfachen eine Reihe von Aufgaben, die auch in der Verwaltung zum Arbeitsinhalt vieler Mitarbeitenden gehören. Sie ermöglichen es den Nutzenden, beispielsweise die KI-Werkzeuge um eine Stellungnahme zu einem bestehenden Text[3] zu bitten oder sie aufzufordern, einen neuen Text zu einem bestimmten Thema zu erstellen.

Diese Werkzeuge sind nicht «intelligent»; sie berechnen z.B. bei der Textgenerierung lediglich die statistische Wahrscheinlichkeit der Wortteilfolge – sie sind also *next token prediction systems* – liefern aber dennoch oft erstaunliche Ergebnisse. Sie werden mit grossen Datenmengen gefüttert, deren Quellen meistens nicht offengelegt sind. Die darauf berechneten Wahrscheinlichkeiten können daher veraltet, irreführend, diskriminierend oder schlicht falsch sein. Ebenso dienen die Eingaben (sog. *Prompts* oder Eingabeaufforderungen) unter Umständen dem weiteren Training des KI-Systems, sie können also in andere Unterhaltungen einfliessen. Die Daten werden in der Regel auch ausserhalb der Schweiz gespeichert.

Verantwortungsvolles Experimentieren? Ja!

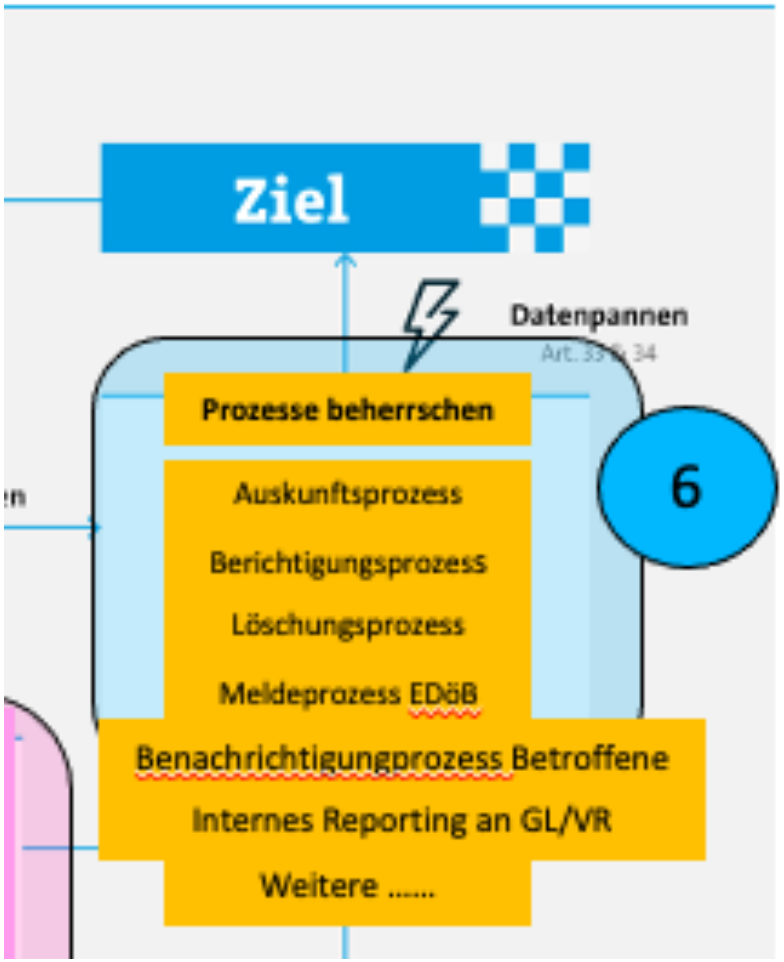
Generative KI-Werkzeuge können Sie bei Ihrer täglichen Verwaltungstätigkeit unterstützen. Probieren Sie es aus, lernen Sie dazu! Mit etwas Kreativität tragen Sie so zu einer innovativen Verwaltung bei.

https://cnai.swiss/wp-content/uploads/2024/01/Merkblatt-zur-Verwendung-von-generativen-KI-Werkzeugen-in-der-Bundesverwaltung_V1.2_DE_clear.pdf

Prozessbeschreibungen

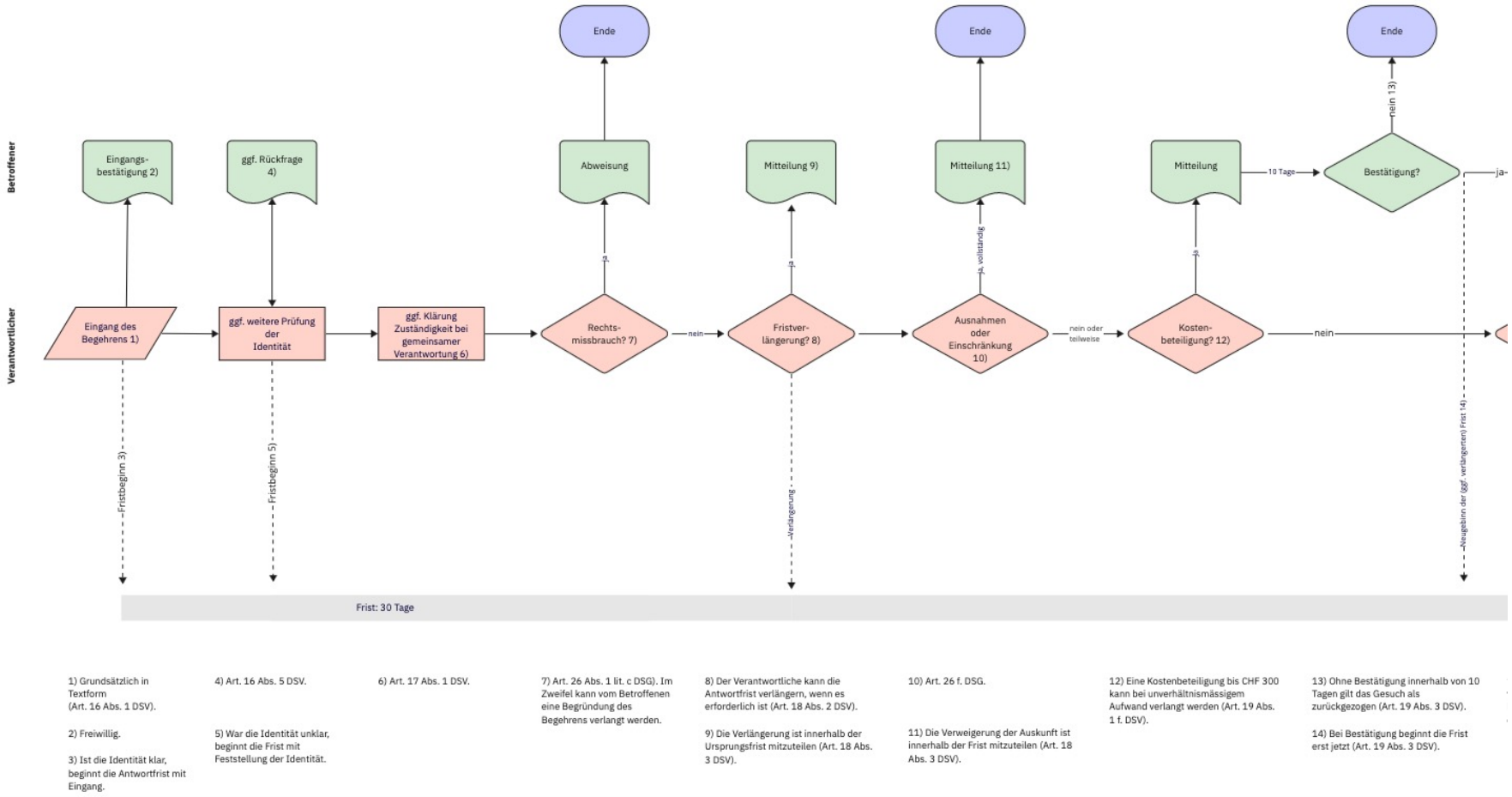
Schritt 6

Prozessbeschreibungen und Prozessbeherrschung für Betroffenenrechte



Wer ISO-basierte QM-Systeme (z.B. ISO9001) im Einsatz hat, bindet diese Zusatzprozesse dort ein.

Beispielauszug: Auskunftsbegehren Personendaten



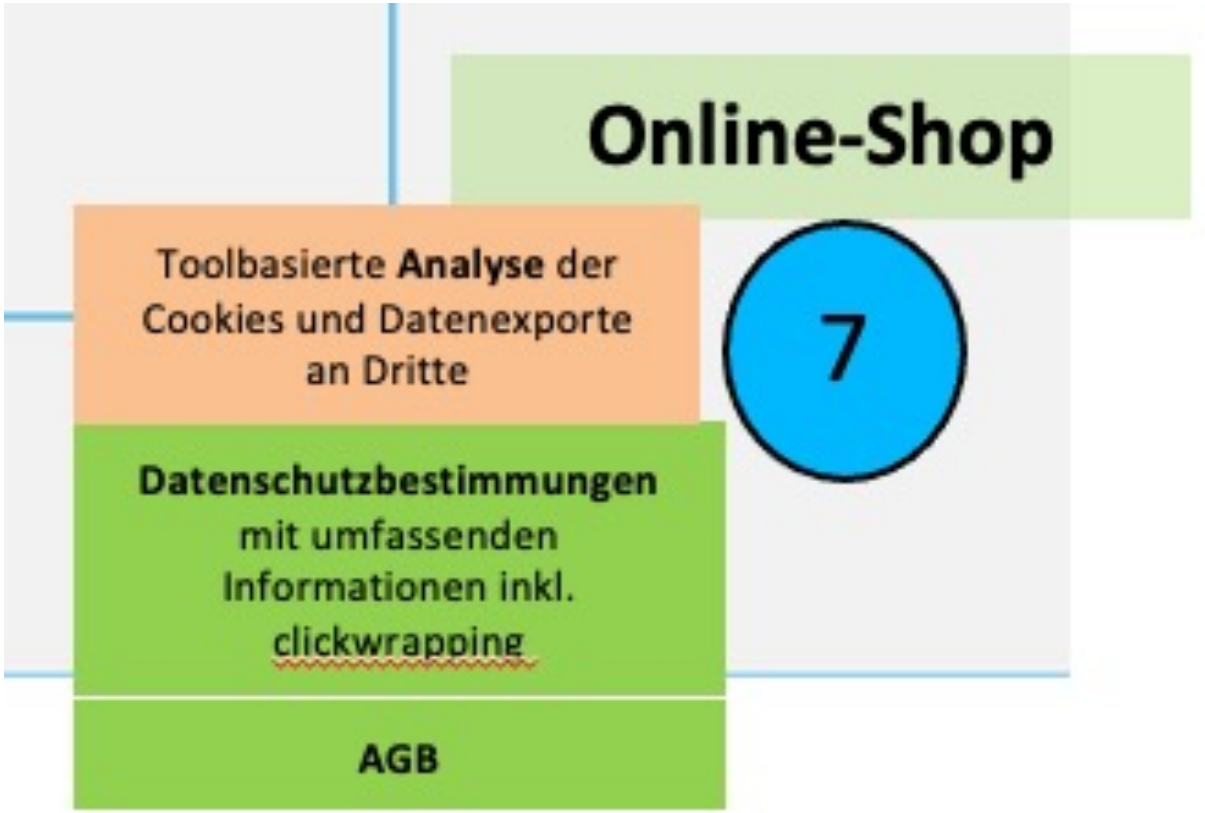
Quelle:
https://datenrecht.ch/wp-content/uploads/230612-Ablauf-Auskunftsbegehren-DSG.pdf

Datenschutzbestimmungen

(Online-Plattformen)

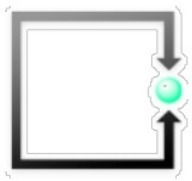
Schritt

Anpassung Datenschutzbestimmungen



Schritt 7
Überprüfung und Anpassung Online-Auftritt (Cookies-Scan)

FSDZ RECHTSANWÄLTE & NOTARIAT AG



Datenschutz Übersicht: Überprüfung der Webseite

Inhaltsverzeichnis

Ist-Zustand

Land	Unternehmen	Produkt und Verbindungs-URL
US	AWIN AG	AWIN https://www.dwin1.com/30129.js
US	Meta Platforms Ireland Limited	Facebook Pixel https://connect.facebook.net/en_US/fbevents.js
US	Google Ireland Limited	Google Ads https://www.googleadservices.com/pagead/conversion_async.js
US	Google Ireland Limited	Google Analytics https://www.google-analytics.com/gtm/optimize.js?id=GTM-P5C25CF
US	Google Ireland Limited	Google CDN https://www.gstatic.com/recaptcha/releases/duyHVVR9Brf6N2GewjkPRfsA/recaptcha__en.js
US	Google Ireland Limited	Google DoubleClick https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j96&tid=UA-11542176-1&cid=551682120.1662465916&jid=2011759994&gjid=2089981837&_gid=186305641.1662465916&_u=YEBAAAAAQAAAAC~&z=2042203877
US	Google Ireland Limited	Google Fonts https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2
US	Google Ireland Limited	Google Tag Manager https://www.google-tagmanager.com/gtm.js?id=GTM-W3LG433
US	Google Ireland Limited	Google reCAPTCHA https://www.google.com/ads/ga-audiences?t=sr&aip=1&_r=4&slf_rd=1&v=1&_v=j96&tid=UA-11542176-1&cid=551682120.1662465916&jid=2011759994&_u=YEBAAAAAQAAAAC~&z=970629497
US	Hotjar Ltd.	Hotjar Behavior Analytics https://vars.hotjar.com/box-

Webseiten-Scan

Zusammenfassung Datenübertragung zu Drittanbietern

Webseiten-Scan

Vorwort

Mithilfe von Cookies können personenbezogene Daten zwischengespeichert werden, wodurch ermöglicht wird, Nutzer zu tracken. Folgende Cookies werden beim Aufruf Ihrer Website (https://shub.ch/) gesetzt.

Ist-Zustand

Domain	Name	Ablaufdatum
shub.ch	01499b3eb6756924e431bcddb05ff4fb	Session

SSL-Zertifikat

Verpflichtendes SSL: Ja

TLS Version: TLS 1.2

Aussteller: Let's Encrypt - US

Zertifikatsname: R3

Gültig von: 11.08.2023

Gültig bis: 09.11.2023

Serverstandort

Ihr Server befindet sich in CH.

Webseiten-Scan

8.1. Cookies, die wir verwenden

Beim Verwenden unserer Website platzieren wir das **Session-Cookie 01499b3eb6756924e431bcddb05ff4fb**. Dieses Session-Cookie wird von Joomla! benötigt, um die Funktionsfähigkeit des Frameworks sicherzustellen. Joomla! Ist ein Open Source Content Management System und dient der Erstellung und der Verwaltung von Webseiten. Session-Cookies sind temporär, haben kein Verfallsdatum und speichern nur Informationen darüber, was der Nutzer während einer einzelnen Sitzung tut. Eine Session ist einfach ein zufällig generierter und eindeutiger Wert, der zugewiesen wird, wenn jemand eine Webseite besucht. Session-Cookies werden vorübergehend im Speicher abgelegt und automatisch entfernt, wenn der Browser geschlossen wird oder die Sitzung endet.

8.2 Google Fonts

Wir verwenden Google Fonts von Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, als Dienst zur Bereitstellung von Schriftarten für unser Onlineangebot. Um diese Schriftarten zu beziehen, stellen Sie eine Verbindung zu Servern von Google Ireland Limited her, wobei Ihre IP-Adresse übertragen wird. Die konkrete Speicherdauer der verarbeiteten Daten ist nicht durch uns beeinflussbar, sondern wird von Google Ireland Limited bestimmt. Weitere Hinweise finden Sie in der Datenschutzerklärung für Google Fonts: https://policies.google.com/privacy.

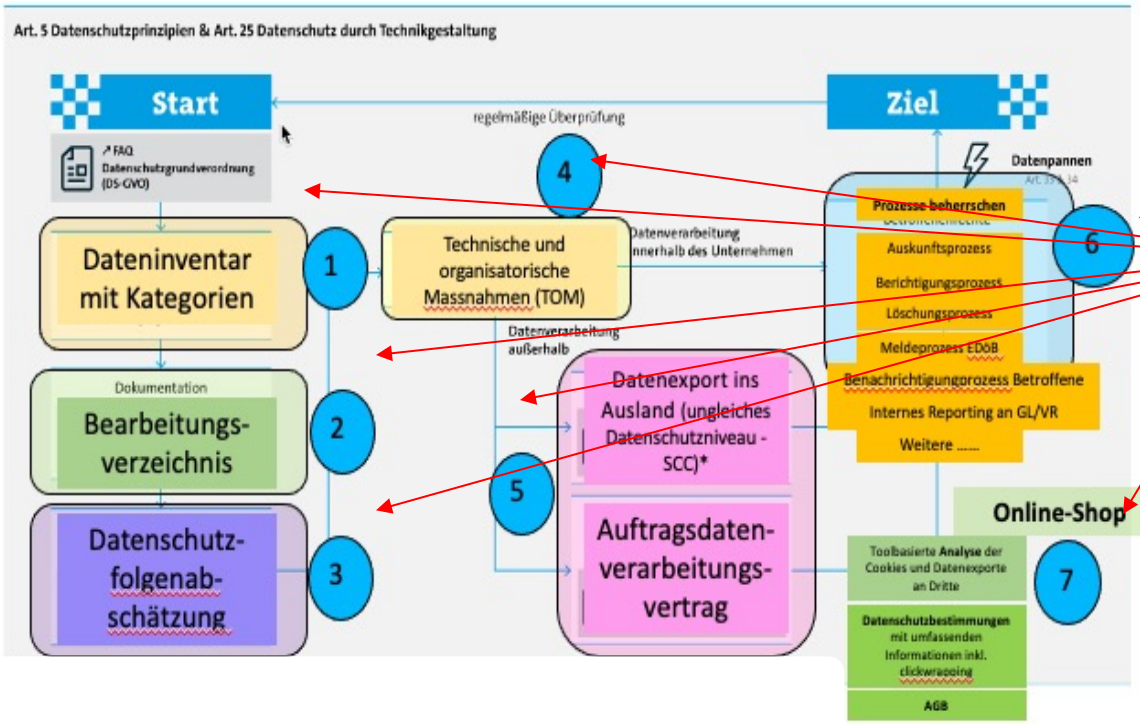
Schritt 7

Überprüfung und Anpassung Online-Auftritt

In der Regel ist eine Anpassung folgender Bereiche eines Webauftritts notwendig:

- Allgemeine Geschäftsbedingungen
- **Separate Datenschutzbestimmungen** mit Detailinformationen zu bearbeiteten Daten, Datenweitergabe und Widerrufsrechte des Betroffenen
- Einbau des Clickwrapping (nachweisbare Einwilligungserklärung des Benutzers) in Webseite oder Profil-Erhebungsseiten
- Sicherstellung des Einhaltung des Koppelungsverbotes (Alternativzugang mit oder ohne Akzept zur Datenbearbeitung einführen)

Unsere Unterstützungsleistungen



Team erarbeitet Entwürfe nach Projektplan

Wir reviewen Ihre Entwürfe und geben Verbesserungs-Feedback

Team passt Entwürfe an und finalisiert diese.

Unternehmen schult seine Mitarbeitenden auf den 1.9.2023

Teil 11:

Bearbeitungsverzeichnis n-DSG

Bettina Schneider

Separate Folienpräsentation
von Dr. Bettina Schneider

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. 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 12:

Datenschutz-Folgenabschätzung (DSFA) nach nDSG

Esther Zaugg

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;

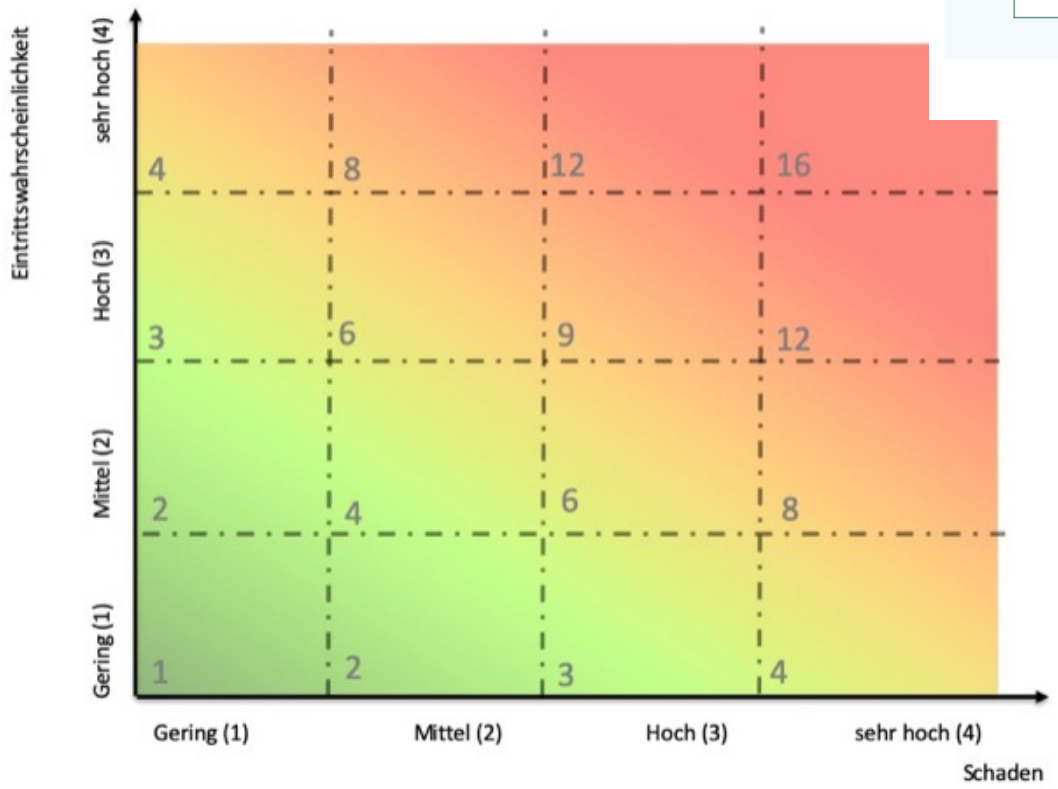
b. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden

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

Praxis-Aufgabe

Lukas Fässler

Ausarbeitung einer Data Protection Policy (auf Stufe VR)

in Gruppenarbeit

Data Protection Policy

Eine Datenschutzpolitik ist eine Erklärung, die darlegt, wie Ihre Organisation personenbezogene Daten schützt.

Es handelt sich um eine Reihe von Grundsätzen, Regeln und Leitlinien, die Auskunft darüber geben, wie Sie die ständige Einhaltung der Datenschutzgesetze sicherstellen werden.

Sie wird im Sinne einer allgemeinen Leitlinie des Verwaltungsrates und/oder der Geschäftsleitung zum Umgang mit Personendaten, besonders schützenswerten Personendaten und Profiling-Daten ausgestaltet. Sie hat Weisungscharakter.

Sie ist so allgemein zu halten, dass die GL oder das Umsetzungsteam, welches mit der Sicherstellung der Datenschutz-Compliance beauftragt wurde, nicht in der konkreten Ausgestaltung der Ergebnisse eingeschränkt wird.

Aufgabe

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

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

Data Protection Policy

Rechtsanwalt Lukas Fässler

Präsentationen in Gruppen
Feedback-Runde

Verzeichnis von Verarbeitungstätigkeiten

Dr. Bettina Schneider

Präsentationen in Gruppen
Feedback-Runde

Datenschutz-Folgeabschätzung

Esther Zaugg

Präsentationen in Gruppen
Feedback-Runde

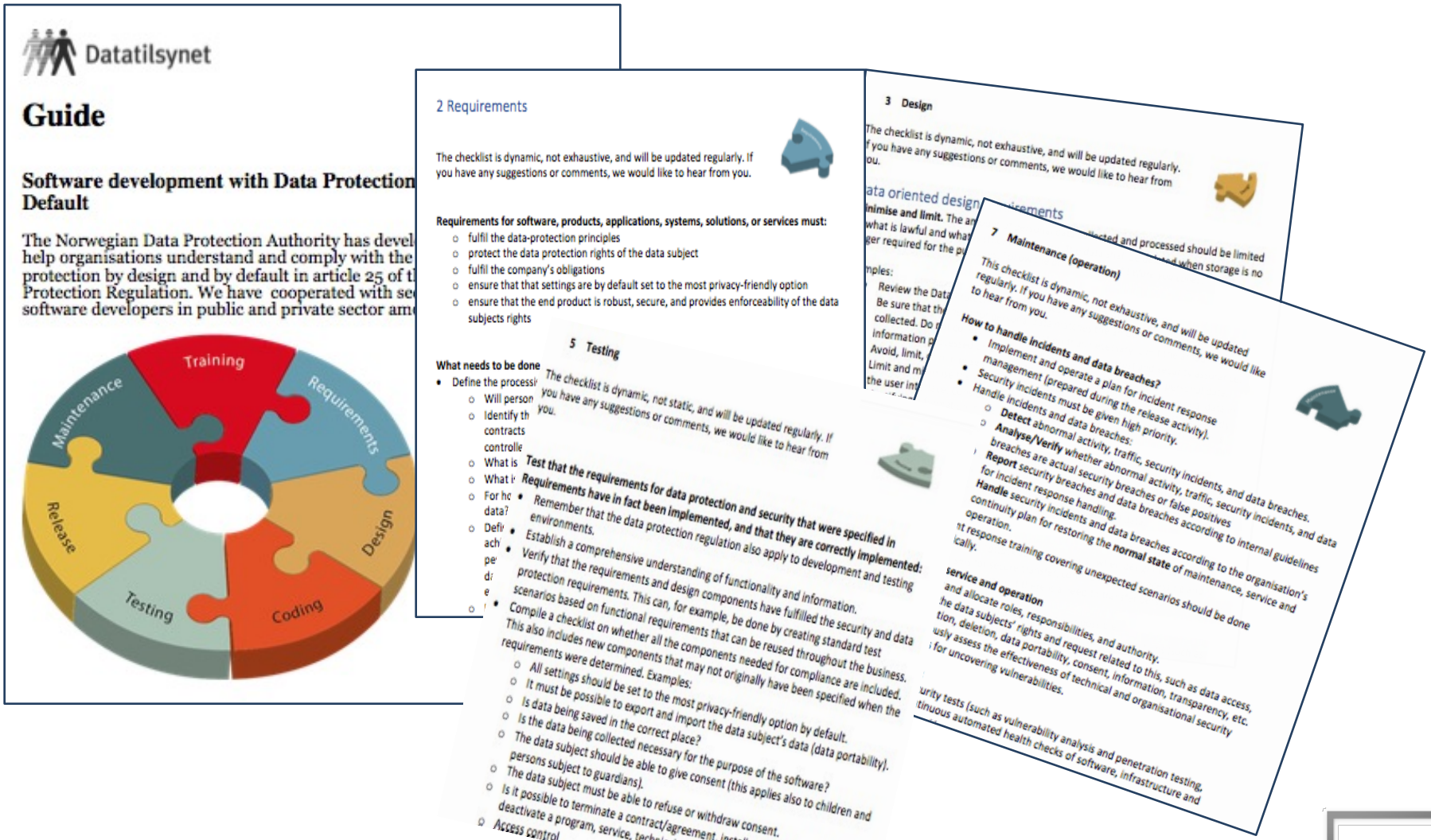
Zusammenfassung und Fragen

Rechtsanwalt Lukas Fässler
Dr. Bettina Schneider
Esther Zaugg

Unterlagen für die Praxis

https://www.bitkom.org

Diverse Checklisten



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

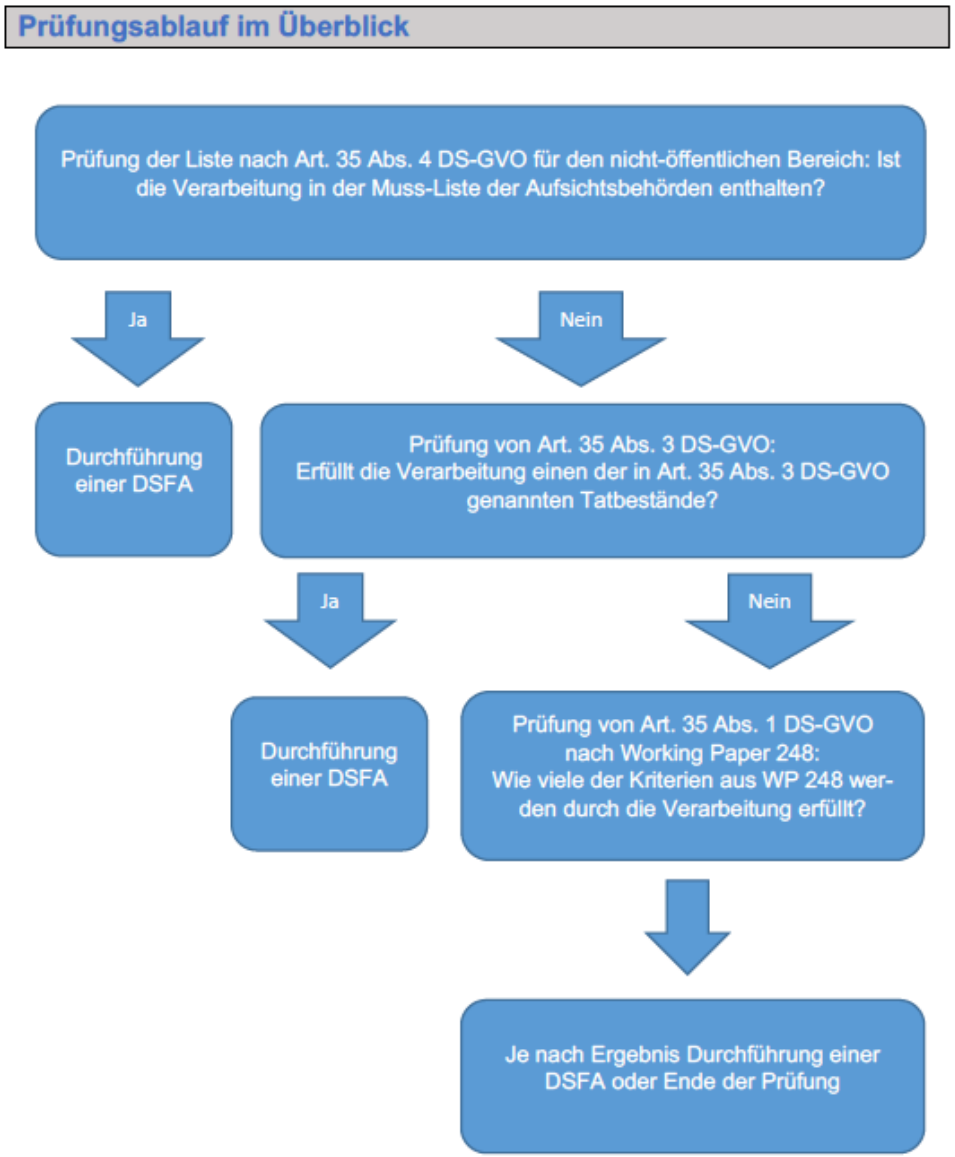
Prüfschema: Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 Datenschutz-Grundverordnung für den nicht-öffentlichen Bereich

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)

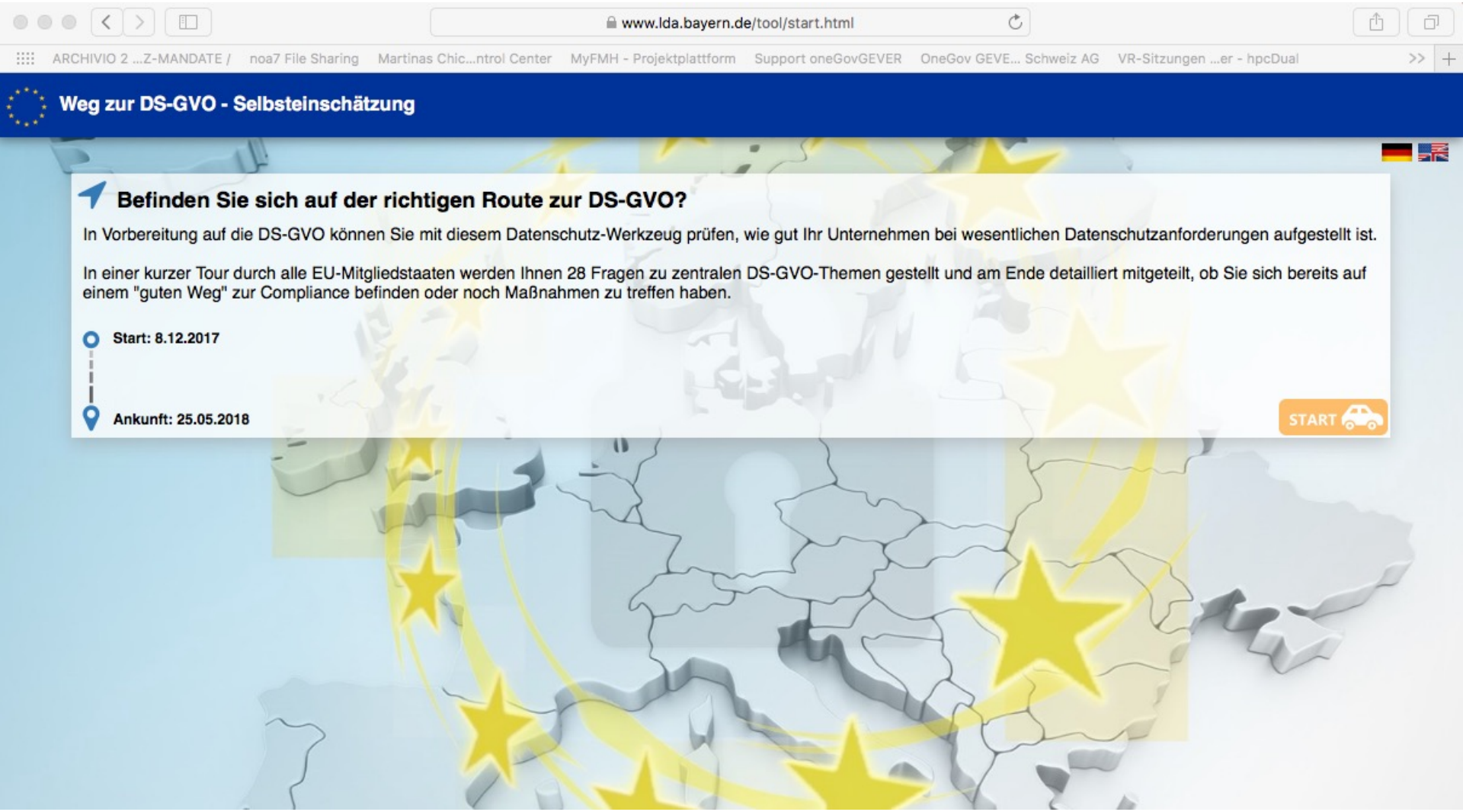


Checkliste

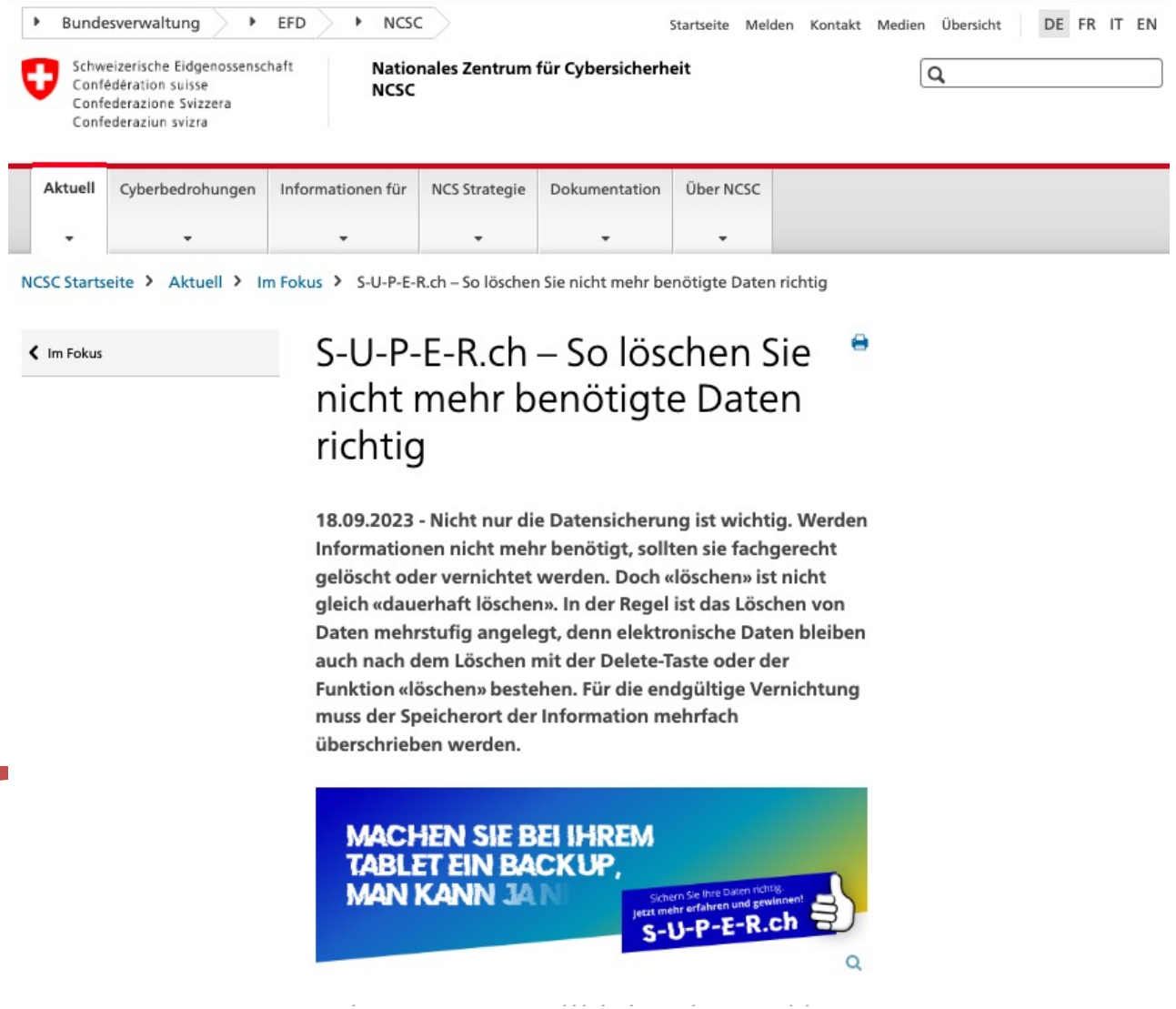
A. Prüfung der Liste nach Art. 35 Abs. 4 DS-GVO		Ja	Nein
A.1	Biometrische Daten zur eindeutigen Identifizierung	☐	☐
A.2	Genetische Daten im Sinne von Artikel 4 Nr. 13 DS-GVO	☐	☐
A.3	Sozial-, Berufs- oder besonderes Amtsgeheimnis	☐	☐
A.4	Daten über den Aufenthalt von natürlichen Personen	☐	☐
A.5	Zusammenführung 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	☐	☐

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

Wie lösche ich Daten richtig



https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/ks-datenloeschung.html

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