

Rechtliche Aspekte



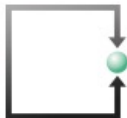
Lukas Fässler

Rechtsanwalt & Informatikexperte

FSDZ Rechtsanwälte & Notariat AG Zug

www.fsdz.ch

faessler@fsdz.ch



Rechtsanwälte
ATTORNEYS @ LAW



Umsetzung der DSGVO

Hinweis schliessen

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



Jetzt anrufen 041 727 60 80
oder E-Mail schreiben

FSDZ Rechtsanwälte & Notariat AG

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

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

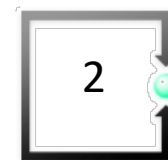
Rechtsanwältin und Notarin
lic. iur. Carmen de la Cruz Böhringer
Telefon +41 41 727 60 80
sekretariat@fsdz.ch

Assoziierte selbständige Anwältin:

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

Partnerkanzlei de la cruz beranek Rechtsanwälte AG, Zug

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





Lukas Fässler

Rechtsanwalt und Informatikexperte, Certified Software Asset Manager IAITAM Inc.

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

Profil

1975 – 1980

Studium an der Universität Fribourg/CH

1982

Anwaltpatent des Kantons Luzern

1982 – 1984

Gerichtsschreiber am Amtsgericht Hochdorf

1984 - 1987

Gerichtsschreiber am Verwaltungsgericht Luzern

1987 - 1992

EDV-Beauftragter im Gerichtswesen Kanton Luzern

1992 - 1997

Informatikchef des Kantons Luzern

1997

Selbständiger Spezialanwalt seit September 1997

1999 - 2000

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

2017

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

Verwaltungsratsmandate

- Verwaltungsratspräsident der FSDZ Rechtsanwälte & Notariat AG Zug
- Verwaltungsratspräsident der e-comtrust International AG, Zug
- Verwaltungsratspräsident AR Informatik AG
- Verwaltungsrat Health Info Net AG (HIN)
- Informatik-Leistungs-Zentrum ILZ der Kantone Obwalden und Nidwalden, Vizepräsident des Verwaltungsrates
- Präsident Verein Schweizerische Städte- und Gemeinde-Informatik SSGi
- Präsident Verein EWML (www.ewml.ch)



Dozententätigkeiten

- **Universität Basel:**
 - Master of Marketing Management, eCommerce-Recht EU und CH
- **Universität Bern/Lausanne:**
 - Master of Advanced Studies for Archival an Information Management
- **Fachhochschule Nordwestschweiz in Basel:**
 - CAS eCommerce und Online-Marketing
 - CAS Information Security & Risk Management
 - CAS IT Service Management & IT Controlling
 - CAS Operational Risk Management
 - Seminar IT Leadership
 - Praxis-Seminar DSGVO und CH E-DSG
 - Seminar öffentliches Beschaffungsrecht
- **Fachhochschule Nordwestschweiz in Olten:**
 - CAS Data und Information Management

Wenn in Europa DataCenters brennen, kommen Fragen der Business Continuity, der Verantwortung und Haftung sofort auf den Tisch



Cloud-Rechenzentrum der OVN in Strassburg am 10.3.2021



Teil 1 Bedrohungslage und Einflussfaktoren

Wie verheerend ein Cyberangriff auf Basis-Infrastrukturen sein kann, hat der Fall der **Colonial Pipeline** im Mai 2021 in den USA gezeigt:

Betreiberfirma musste Rohrleitung abschalten

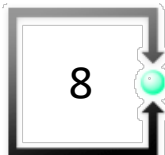
Benzinversorgung an der Ostküste wurde knapp

Ransomware-Angriff mit Systemverschlüsselung und Lösegeld-Erpressung

Hacker dringen durch Sicherheitslücken in IT-Systeme der Unternehmung ein und verschlüsseln und kopieren wichtige Daten. Für Herausgabe des Schlüssels verlangen sie ein Lösegeld (primär in Bitcoins). Oftmals drohen die Täter auch mit der Veröffentlichung von sensiblen (Kunden- oder Geschäfts-) Daten.

Es wurden 4.4 Mio Dollar Lösegeld bezahlt

<https://www.tagesschau.de/wirtschaft/unternehmen/colonial-pipeline-loesegeld-hacker-angriff-ransomware-101.html>



FBI nimmt Pipeline-Hackern Lösegeld ab

Der Hackerangriff auf die größte Benzin-Pipeline hat die Verletzlichkeit der US-Infrastruktur offengelegt. Immerhin wurde den Erpressern nun ein Teil ihrer Beute abgejagt.

Der stellvertretende FBI-Direktor Paul Abbate erläuterte das Verfahren: Das in der [Digitalwährung Bitcoin](#) gezahlte Lösegeld sei bei der Überprüfung zahlloser anonymer Transaktionen in einer digitalen Geldbörse (Wallet) aufgespürt worden. 75 Bitcoin - nach damaligem Wert 4,4 Millionen Dollar - hatte das Versorgungsunternehmen Colonial Pipeline den Hackern bezahlt. 63,7 Bitcoin davon konnte das FBI beschlagnahmen - wegen des Absturzes der digitalen Währung in den vergangenen Wochen mit einem heutigen Wert von 2,3 Millionen Dollar. Es ist das erste Mal, dass eine eigens zum Einsatz gegen Ransomware und digitale Erpressung gegründete Einheit des Ministeriums Lösegeld beschlagnahmt hat.

"Das war ein Angriff auf eine unserer wichtigsten nationalen Infrastrukturen", sagte Lisa Monaco. Hinter der Tat vermutet die US-Regierung [Hacker der Gruppe DarkSide](#) aus Russland.



Cyberangriff auf Comparis

Comparis-Hacker hatten Zugang zu Nutzerdaten

Donnerstag, 15.07.2021, 03:24 Uhr
Aktualisiert um 08:28 Uhr

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

Hackerangriff auf die Rothenburger Auto AG Group

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

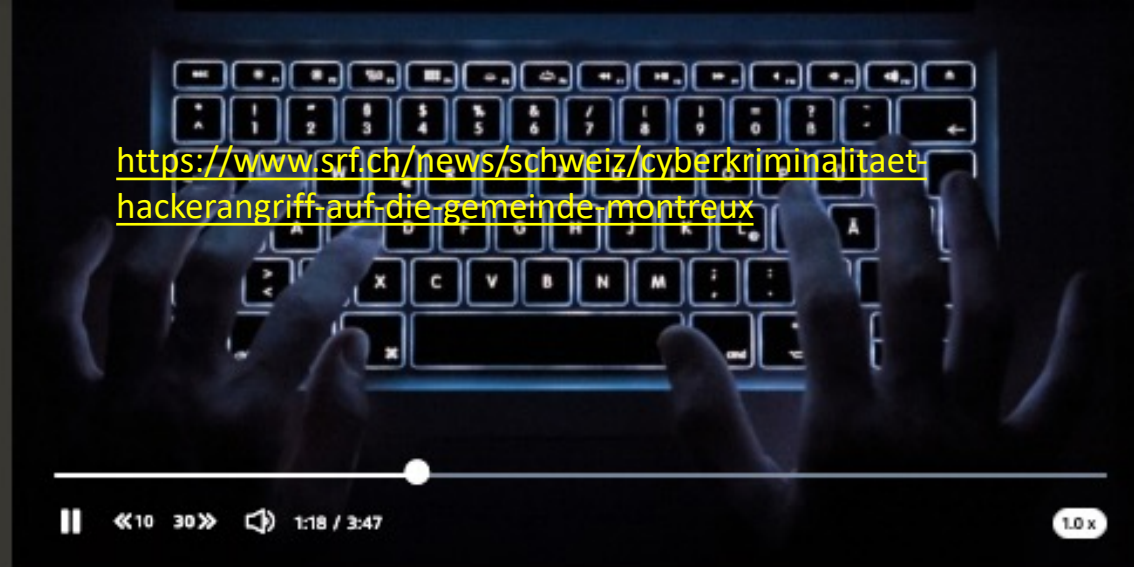
27.08.2019, 17.26 Uhr

Merken Drucken Teilen



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

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



SRF-Digitalredaktor Reto Widmer zum Hackerangriff

Aus SRF 4 News aktuell vom 11.10.2021.

News >

Schweiz >

Quelle:

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

Cyberkriminalität

Hackerangriff auf die Gemeinde Montreux

Montag, 11.10.2021, 08:17 Uhr

Aktualisiert um 11:33 Uhr



Dieser Artikel wurde 4-mal geteilt.

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



Ausweitung der Untersuchungstätigkeit auf die Xplain AG

**Bern, 14.07.2023 - Der EDÖB weitet seine
Untersuchungstätigkeit auf die Xplain AG aus.**

Gemäss seiner Pressemitteilung vom 21. Juni 2023 hat der EDÖB am 20. Juni 2023 eine formelle Untersuchung gegen die Bundesämter für Polizei sowie Zoll- und Grenzsicherheit unter anderem wegen der im Zusammenhang mit der Xplain AG angezeigten Verletzung der Datensicherheit eröffnet.

Inzwischen hat der EDÖB von weiteren Informationen zu diesem Vorfall Kenntnis genommen, die ihn dazu bewogen haben, seine Untersuchungstätigkeit am 13. Juli 2023 auf die Firma Xplain auszudehnen.

CYBERATTACKEN

Vor Bürgenstock-Konferenz: Zahl der russischen Hackerangriffe auf Schweizer Computer nimmt massiv zu



Teilen



Merken



Drucken



Kommentare



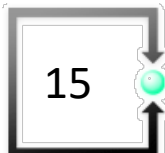
Google News

Seit der Ankündigung der Ukraine-Friedenskonferenz auf dem Bürgenstock ist die Zahl russischer Cyberangriffe rasant angestiegen.

Teil 1

Grundsätze der Unternehmensführung

Das Unternehmen



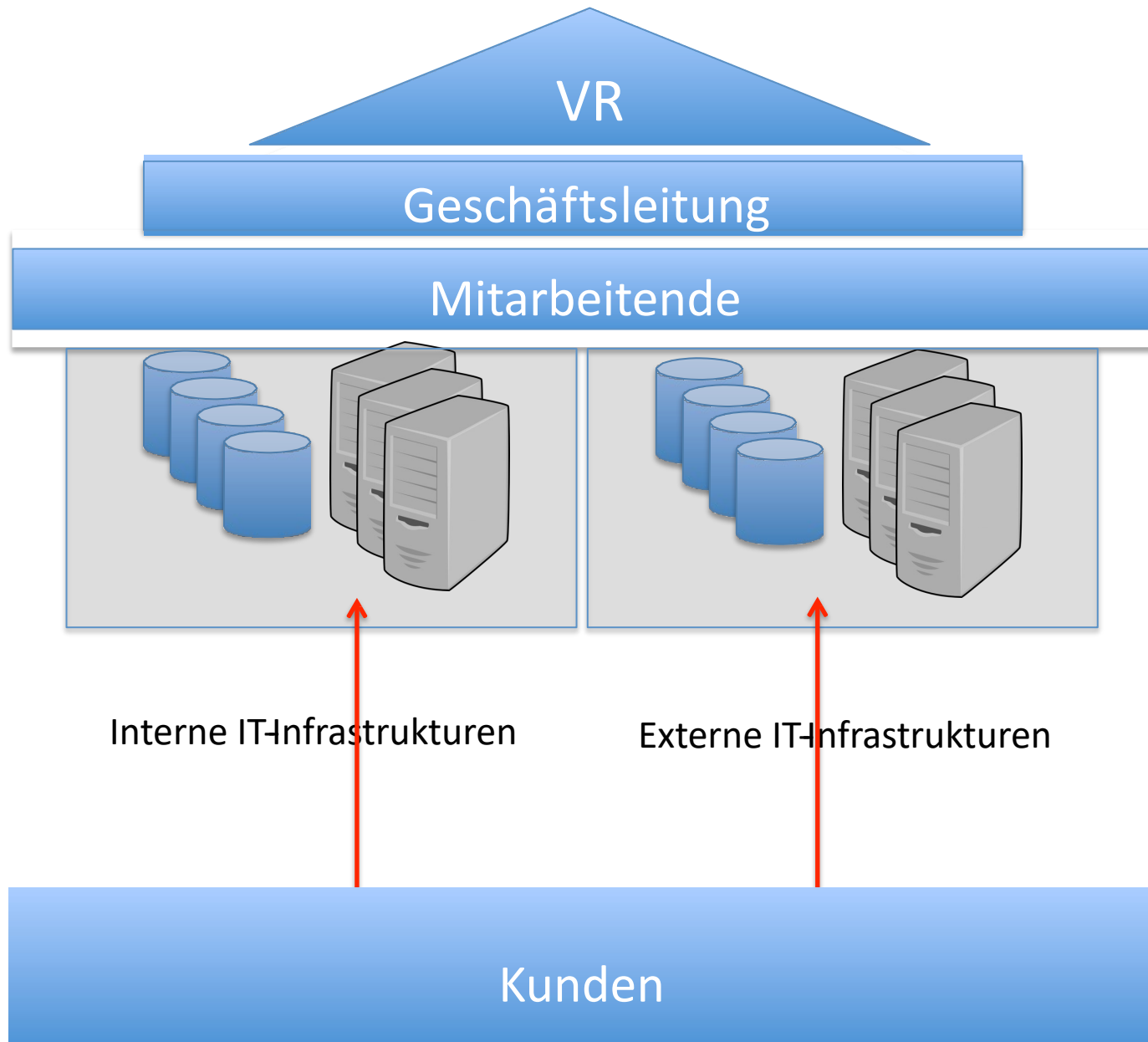
VR - Verwaltungsrat
Strategische Führung

Unternehmung

GL – Geschäftsleitung
Operative Führung

Mitarbeitende
Leistungserbringende

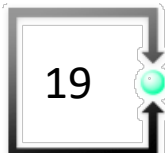
Aktionäre – Aktionariat
Oberstes Organ

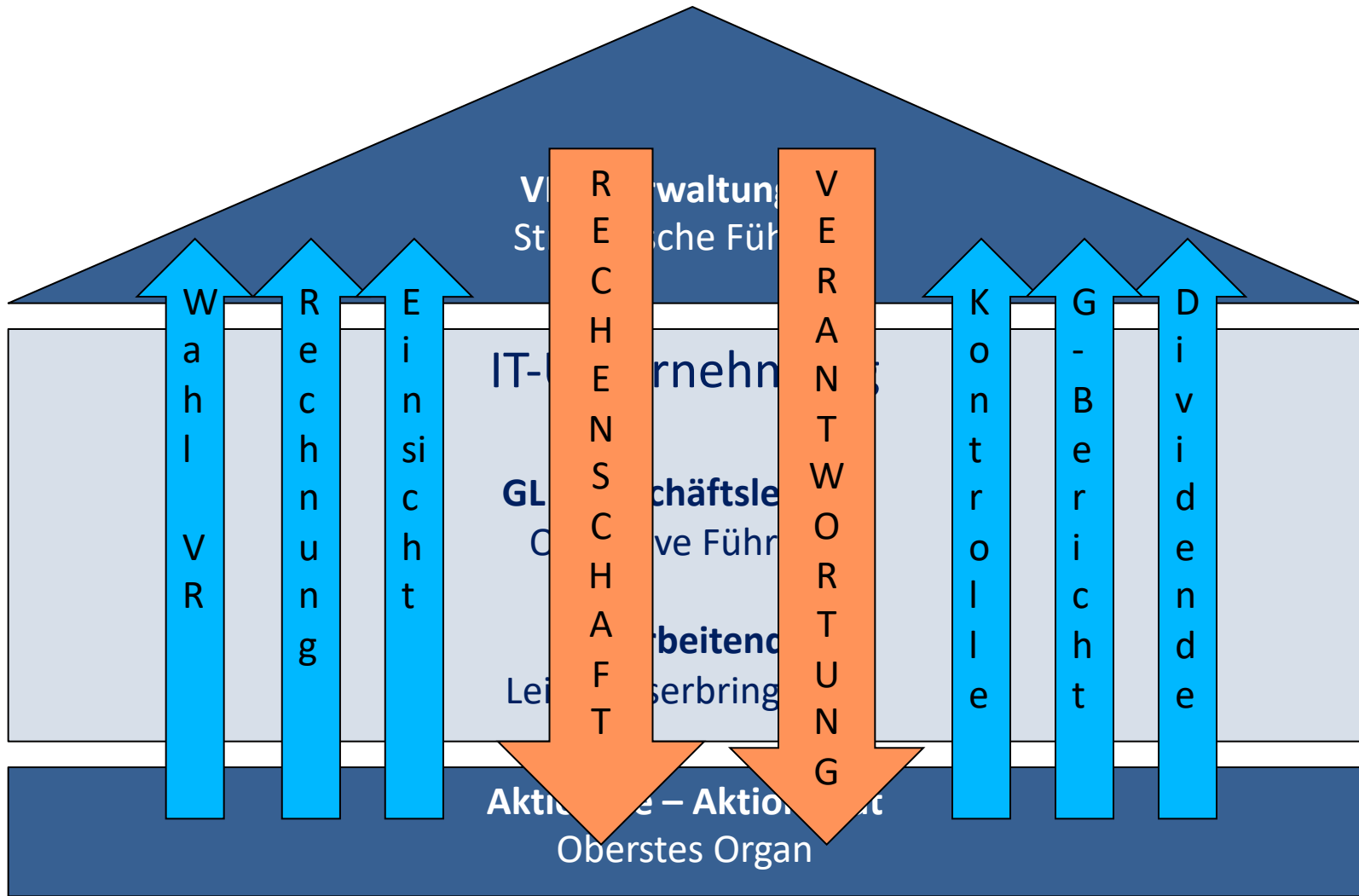


Die gesetzlichen Grundlagen zur Unternehmensführung

Die Generalversammlung der Aktionäre

Aktionäre – Aktionariat
Oberstes Organ





Dritter Abschnitt: Organisation der Aktiengesellschaft

A. Die Generalversammlung

Art. 698

I. Befugnisse

¹ Oberstes Organ der Aktiengesellschaft ist die Generalversammlung der Aktionäre.

² Ihr stehen folgende unübertragbare Befugnisse zu:

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

Aktionäre – Aktionariat
Oberstes Organ

Zweiter Abschnitt: Rechte und Pflichten der Aktionäre

Art. 660³²⁴

A. Recht auf
Gewinn- und
Liquidations-
anteil

I. Im
Allgemeinen

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

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

Aktionäre – Aktionariat
Oberstes Organ



VR - Verwaltungsrat
Strategische Führung

Der Verwaltungsrat **Oberste strategische Führung**

VR - Verwaltungsrat Strategische Führung

Art. 716a⁴³⁰

2. Unübertragbare Aufgaben

¹ Der Verwaltungsrat hat folgende unübertragbare und unentziehbare Aufgaben:

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes⁴³¹ sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

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

VR - Verwaltungsrat
Strategische Führung

B. Der Verwaltungsrat⁴¹⁴

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

Compliance-Verantwortung

VR - Verwaltungsrat Strategische Führung

B. Der Verwaltungsrat⁴¹⁴

Art. 717⁴³³

IV. Sorgfalts-
und Treuepflicht

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

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

Sorgfaltspflichten innerhalb öffentlicher Verwaltungen

20

**Gesetz
über die Organisation von Regierung und Verwaltung**
(Organisationsgesetz, OG)

Beispiel: Kanton Luzern

§ 1 Aufgaben

¹ Der Regierungsrat erfüllt als Kollegialbehörde die ihm in Verfassung und Gesetz zugewiesenen Aufgaben. Die Regierungstätigkeit hat den Vorrang vor den andern Aufgaben des Regierungsrates und seiner Mitglieder.

² Von den Verwaltungsaufgaben, die durch die Rechtsordnung nicht einem bestimmten Verwaltungsorgan übertragen sind, erfüllt der Regierungsrat die wichtigsten selbst. Die andern überträgt er den Departementen, der Staatskanzlei, den Dienststellen oder andern Verwaltungsorganen.

§ 21 Grundsätze der Aufgabenerfüllung *

¹ Die Verwaltung handelt rechtmässig und richtet ihr Handeln auf die Erfüllung der gesetzlichen Ziele und der Leistungsaufträge aus. Sie verwendet die öffentlichen Mittel wirtschaftlich und wirksam. *

a. * ...

§ 21a * Grundsätze der Verwaltungsführung

¹ Der Regierungsrat und seine Mitglieder führen die Verwaltung, indem sie

- a. die bedeutenden Entwicklungen und Risiken beurteilen und die politischen Schwerpunkte setzen,
- b. im Rahmen der Rechtsordnung die wesentlichen Ziele und Mittel der Verwaltung festlegen und Prioritäten setzen,
- c. für eine zweckmässige Delegation von Aufgaben, Kompetenzen und Verantwortlichkeiten sorgen,
- d. die regelmässige Überprüfung der Leistungsaufträge und der Leistungserbringung der Verwaltung sicherstellen.

² Sie regeln Geschäftsprozesse und Organisation, passen sie veränderten Verhältnissen an und setzen geeignete Führungsinstrumente ein.

³ Sie stellen ein systematisches, insbesondere auf die festgelegten Ziele und die Risiken der Verwaltungstätigkeit ausgerichtetes Controlling sicher.

§ 21b * Informations-, Geschäftsverwaltungs- und Dokumentationssysteme, Datenbearbeitung

¹ Die Verwaltung führt zur Erfüllung ihrer gesetzlichen Aufgaben elektronische Informations-, Geschäftsverwaltungs- und Dokumentationssysteme.

² Sie bearbeitet Personendaten und Angaben über juristische Personen und Personengesellschaften des Handelsrechts sowie Sachdaten im Rahmen ihrer Aufgabenerfüllung. Vorbehalten bleiben die Bestimmungen der Datenschutz-, der Informatik- und der Archivgesetzgebung.

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

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

III. Haftung für
Verwaltung,
Geschäfts-
führung und
Liquidation

Art. 754⁴⁸⁸

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

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



Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Urteilkopf

139 III 24

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

Regeste a

Art. 754 OR; aktienrechtliche Verantwortlichkeit.

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



Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

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

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

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

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

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

III. Haftung für
Verwaltung,
Geschäfts-
führung 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

Treuepflicht des Arbeitnehmers

II. Sorgfalts- und Treuepflicht

Art. 321a

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.

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



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

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



Einfluss von Standards und Normen



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

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

Art. 962 OR

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



swiss code of best practice for corporate governance

Swiss Code of Best Practice

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



Aufgaben des Verwaltungsrats

9

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

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



Umgang mit Risiken und Compliance, internes Kontrollsystem

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

20

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



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.

Nationale Minimal-Standards, Normen und Empfehlungen zur Cyber-Sicherheit

Startseite

Wirtschaftliche
Landesversorgung

Themen

Dokumente

Kontakt und
Dienstleistungen

Startseite > Themen > IKT

← Themen

IKT

IKT-Minimalstandard

NCS-Strategie

IKT



Informations- und Kommunikationstechnologien (IKT) sind für Unternehmen unabdingbar geworden. Sie durchdringen alle Branchen, was sich positiv auf Produktivität und Effizienz der Wirtschaft auswirkt. Sollte die Telekommunikation grossflächig ausfallen, wäre die Funktionsfähigkeit der Wirtschaft gefährdet.

SMIDEX SUISSE
Smart ID Exposyum

Aktuell

**Kritische Infrastrukturen besser schützen vor
Cyber-Angriffen**

Cyber-Bedrohungen, Cyber-Risiken und Wege sich davor zu schützen, standen im Zentrum der SMIDEX-Konferenz in Zürich vom 17. und 18. November. Das BWL, welches die Konferenz am Mittwoch mit eröffnet



Wirtschaftliche
Landesversorgung

Themen

Dokumente

Kontakt und
Dienstleistungen

Startseite > Themen > IKT > IKT-Minimalstandard > Branchenstandards

← IKT-Minimalstandard

Branchenstandards

Wasserversorgung

Abwasser

Lebensmittel

Gasversorgung

Öffentlicher Verkehr

Strom

Branchenstandards



Der IKT-Minimalstandard dient als Empfehlung und mögliche Richtschnur zur Verbesserung der IKT-Resilienz. Er richtet sich insbesondere an die Betreiber von kritischen Infrastrukturen, ist aber grundsätzlich für jedes Unternehmen oder jede Organisation anwendbar und frei verfügbar.

Um die Anwendung dem Minimalstandard in kritischen Sektoren zu erleichtern, hat die wirtschaftliche Versorgung in Zusammenarbeit mit den Branchenverbänden der betroffenen Sektoren den Minimalstandard festgelegt, um den Besonderheiten ihres Sektors Rechnung zu tragen. Diese Arbeit hat zur Entwicklung von Minimalstandards für die verschiedenen Sektoren der WL geführt.

Letzte Änderung 07.01.2021

[^ Zum Seitenanfang](#)



Bundesamt für wirtschaftliche Landesversorgung BWL



<https://www.youtube.com/watch?v=mdr2FPo1W1o>



Minimalstandard zur Verbesserung der IKT-Resilienz

https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
**Bundesamt für wirtschaftliche
Landesversorgung BWL**

www.bwl.admin.ch

Herzlich Willkommen

im Nationalen Zentrum
für Cybersicherheit NCSC



Informationen für



Privatpersonen

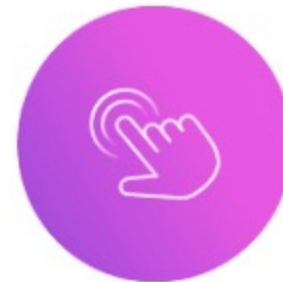


Unternehmen



IT-Spezialisten

Melden Sie uns



einen
Cybervorfall



eine
Schwachstelle

<https://www.ncsc.admin.ch/ncsc/de/home.html>



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE
Digital Innovation Office

Bericht vom 28 Juni 2021

Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung

Datum: 28 Juni 2021

Ort: Bern

Auftraggeberin:

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

Auftragnehmer/in:

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

Feststellungen mit Adressierung der Sorgfaltspflichten

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

Weitere Richtlinien

- IKT-Minimalstandard“ des BA für wirtschaftliche Landesversorgung (BWL)
- Handbuch Grundschutz für Operational Technology des Branchenverbandes Schweizer Elektrizitätswirtschaft (VSE)
- Nationale Strategie zum Schutz vor Cyber-Risiken (NCS) seit 2021, für die Periode 2018-2022 wesentlich ausgeweitet.

Quelle: Bundesamt für Energie – Bericht vom 28.6.2021, S. 11 ff.

Administrative Analysevorgaben

Risiko- und Schutzbedarfsanalyse für Smart Grids (2016a)

Herausgeber: BFE, OFFIS – Institut für Informatik, Josef Ressel Zentrum FH Salzburg & ecofys

Risiko- und Schutzbedarfsanalyse für Smart Meter (2016b)

Herausgeber: BFE & AWK Group

Risiko- und Verwundbarkeitsanalyse des Teilsektors Stromversorgung (2017)

Herausgeber: BWL

Quelle: Bundesamt für Energie – Bericht vom 28.6.2021, Anhang 3 – Risiko- und Schutzbedarfsanalysen, S. 185 ff.

Nationale Cyberstrategie NCS



Die Cybersicherheit ist auf allen Ebenen ein entscheidendes Element geworden. Sie ist ein Schlüsselement der Sicherheitspolitik, unabdingbare Voraussetzung für die Digitalisierung, Chance für den Wirtschafts- und Forschungsstandort Schweiz sowie ein zunehmend wichtiges Element der Aussenpolitik. Sie betrifft aber nicht nur diese staatspolitischen Themen, sondern ist längst ein Faktor des täglichen Umgangs aller Bürgerinnen und Bürger mit digitalen Technologien geworden. Daraus ergibt sich, dass eine nationale Cybersicherheitsstrategie ein breites Spektrum an Themen und Massnahmen berücksichtigen muss.



Vision

Die Schweiz nutzt die Chancen der Digitalisierung und mindert Cyberbedrohungen und deren Auswirkungen durch geeignete Schutzmassnahmen. Sie gehört zu den weltweit führenden Wissens-, Bildungs- und Innovationsstandorten in der Cybersicherheit. Die Handlungsfähigkeit und die Integrität ihrer Bevölkerung, ihrer Wirtschaft, ihrer Behörden und der in der Schweiz ansässigen internationalen Organisationen gegenüber Cyberbedrohungen sind gewährleistet.

Aktuell

☰ Alle



Der Bundesrat und die Kantone legen die neue Nationale Cyberstrategie fest

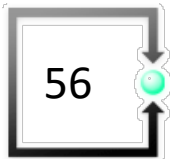
13.04.2023 - Die neue Nationale Cyberstrategie (NCS) wurde an der Sitzung vom 5. April 2023 durch den Bundesrat und an der heutigen Plenarversammlung der KKJPD durch die Kantone gutgeheissen. Die Strategie zeigt auf, mit welchen Zielen und Massnahmen der Bund und die Kantone gemeinsam mit der Wirtschaft und den Hochschulen den Cyberbedrohungen begegnen wollen. Für die Planung und Koordination der Umsetzung wird wiederum ein Steuerungsausschuss eingesetzt, der die Strategie auch weiterentwickeln soll. Dazu soll dessen Rolle ausgebaut und die Unabhängigkeit gestärkt werden.

 [Nationale Cyberstrategie NCS](#)
(PDF, 1 MB, 13.04.2023)

Zug

Gesetzliche Grundlagen zur IT-Sicherheit

Strafrecht



Strafrecht/Cybercrime

- Straftatbestände

Computerdelikte/Cybercrime

- Unbefugte Datenbeschaffung Art. 143 StGB
- Unbefugtes Eindringen in ein Datenverarbeitungssystem Art. 143bis StGB
- Datenbeschädigung Art. 144bis StGB
- Betrügerischer Missbrauch einer Datenverarbeitungsanlage Art. 147 StGB
- Check- und Kreditkartenmissbrauch Art. 148 StGB
- Erschleichen einer Leistung (Art. 150 StGB)
- Herstellen und in Verkehrbringen von Materialien zur unbefugten Entschlüsselung codierter Angebote (Art. 150bis StGB)
- Spamverbot (Art. 45a FMG/ 83 FDV)

Art. 143

Unbefugte
Daten
beschaffung

1 Wer in der Absicht, sich oder einen anderen unrechtmässig zu bereichern, sich oder einem anderen elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt **und gegen seinen unbefugten Zugriff besonders gesichert** sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

2 Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Offizialdelikt: wird von Amtes wegen verfolgt. Es genügt eine Anzeige

Art. 143bis

Unbefugtes
Eindringen in ein
Daten-
verarbeitungssystem

¹Wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, **gegen seinen Zugriff besonders gesichertes** Datenverarbeitungssystem eindringt, wird, **auf Antrag**, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

²Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz I verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Antragsdelikt: Strafuntersuchung muss innerhalb von 3 Monaten nach Kenntnis des Vorfalls mittels Strafantrag vom Opfer initialisiert werden.

Art. 144bis

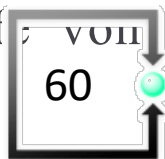
Daten
beschädigung

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird **auf Antrag**, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Hat der Täter einen **grossen Schaden** verursacht, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden. Die Tat wird **von Amtes wegen** verfolgt.

2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Handelt der Täter **gewerbsmässig**, so kann auf Freiheitsstrafe von einem Jahr bis zu fünf Jahren erkannt werden.



Identitätsmissbrauch

Schweizerisches Strafgesetzbuch



Art. 179decies 242

Seit 1.9.2023 in Kraft

Identitätsmiss-
brauch

Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder um sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird auf Antrag mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.

- Die Identität eines Menschen ist durch verschiedene konstituierende Merkmale bestimmbar, etwa durch seinen Namen, seine Herkunft, sein Bild, die soziale, familiäre oder berufliche Positionierung, sowie durch andere persönliche Daten wie Geburtsdatum, Internetadresse, Kontonummer oder Nickname.
- Die Verwendung einer Identität aus reinem Übermut oder als Scherz fällt damit nicht unter die Bestimmung. Die Verwendung einer neuen, fiktiven Identität fällt ebenso wenig in den Anwendungsbereich
- Der in der Strafbestimmung statuierte Nachteil für den durch den Identitätsmissbrauch Betroffenen muss eine gewisse Schwere erreichen und kann materieller oder immaterieller Natur sein.
- Die Absicht, beim Betroffenen einen massiven Ärger auszulösen, kann als Nachteilsabsicht bereits ausreichen.

Beispiel

Diebstahl Halterdaten

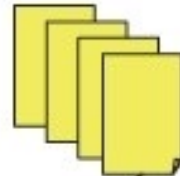


█ gibt Autonummern einen Namen: Wer einen Autohalter personalisieren möchte, dem bietet sich ab sofort für CHF 0.80 pro Anfrage eine neue Möglichkeit. █ ist eine vollautomatische Plattform, welche die rasche Abfrage der Fahrzeughalterdaten per SMS ermöglicht: Autokennzeichen eintippen, SMS an █ senden und innerhalb weniger Sekunden erscheint die Antwort auf dem Display. Einfacher und schneller geht es nicht. Vorerst bietet █ den Dienst für die folgenden acht Kantone an: BL, LU, NE, NW, OW, TI, VS und ZG. Weitere sollen bald folgen.

Strassenverkehrsämter



Haftpflichtversicherer



Versicherungsnachweise



Bootnetz in Hanoi/Vietnam



1



2



2 INVESTIGATIVE FINDINGS

2.1 Intrusion Timeline

InfoGuard established the following timeline in Table 1. based on investigative results. InfoGuard lists all timestamps in Universal Coordinated Time (UTC)

DATE	EVENT
2020-04-14	Execution of CopyData.exe and Upload.cmd on TS99
2020-04-23	Execution of UploadBackup.exe and Upload.cmd in a TeamViewer session on TS97
2020-04-30	Execution of UploadBackup.exe on TS99
2020-06-12	Execution of UploadBackup.exe in a TeamViewer session on TS97
2020-06-30	Execution of UploadBackup.exe, Notepad.exe and cmd.exe in a TeamViewer session on TS97
2020-07-01	The Attacker had a TeamViewer Session on TS97
2020-07-02	Two TeamViewer sessions, in the second was UploadBackup.exe and Notepad.exe executed on TS97
2020-08-12	Execution of UploadBackup.exe in a TeamViewer session on TS82

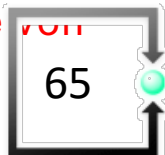
Abteilung I

Präsident Trüb, Amtsrichterinnen Unternährer, Meier und Ersatzrichter Dätwyler, Gerichtsschreiberin Wigger

Urteil vom 6. Dezember 2010

Rechtsspruch

1. M W ist schuldig der mehrfachen unbefugten Datenbeschaffung nach Art. 143 Abs. 1 StGB, begangen in mittelbarer Täterschaft vom 20.5.2008 bis 31.7.2008.
2. M W wird in Anwendung von Art. 34, Art. 42 Abs. 1, Art. 44 Abs. 1, Art. 47, Art. 49 Abs. 1 und Art. 51 StGB mit einer **Geldstrafe von Fr. 8'800.00, 80 Tagessätzen zu je Fr. 110.00** bestraft unter Anrechnung von zwei Tagessätzen erstanden aus der zweitägigen Untersuchungshaft vom 19.11.2008 bis 20.11.2008. Die **Geldstrafe wird bedingt ausgesprochen bei einer Probezeit von 2 Jahren.**
3. Zusätzlich wird in Anwendung von Art. 42 Abs. 4 und Art. 106 StGB eine **Busse von Fr. 1'750.00** ausgesprochen. Die Ersatzfreiheitsstrafe beträgt 16 Tage.





1B_59/2021

Urteil vom 18. Oktober 2021

I. öffentlich-rechtliche Abteilung

Besetzung

Bundesrichter Kneubühler, Präsident,
Bundesrichter Chaix, Bundesrichterin Jametti,
Bundesrichter Haag, Bundesrichter Merz,
Gerichtsschreiberin Dambeck.

Verfahrensbeteiligte

A. _____,
Beschwerdeführer,
vertreten durch Rechtsanwältin Dr. Karen Schobloch,

gegen

Staatsanwaltschaft II des Kantons Zürich,
Abteilung Schwerpunktkriminalität,
Cybercrime und Besondere Untersuchungen,
Selnaustrasse 32, Postfach, 8027 Zürich.

Gegenstand

Vorzeitige Verwertung / Beschlagnahme
des Verwertungserlöses,

Beschwerde gegen den Beschluss des Obergerichts
des Kantons Zürich, III. Strafkammer,
vom 22. Dezember 2020 (UH200287-O/U/BEE).

1B_59/2021: Verwertung beschlagnahmter Kryptobestände (amtl.
Publ.)

Im Urteil 1B_59/2021 vom 18. Oktober 2021
äusserte sich das Bundesgericht erstmals zum

gebotenen Vorgehen der Staatsanwaltschaft
bei der Verwertung beschlagnahmter Kryp-
tobestände. Aufgrund des dafür erforderlichen
Fachwissens muss die Staatsanwaltschaft
Vorkehrungen treffen, um bei der vorzeitigen
Verwertung beschlagnahmter kryptobasierter
Vermögenswerte ein möglichst gutes Ergebnis
zu erzielen. Sofern das nötige Fachwissen
dazu in der Behörde nicht vorhanden ist, muss
sie eine Fachperson beiziehen.

Teil 3

Grundsätze des neuen Datenschutz- und Datensicherheitsrechts

Bundesverfassung der Schweizerischen Eidgenossenschaft

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

Art. 13 Schutz der Privatsphäre

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

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

vom 10. Dezember 1907 (Stand am 1. Juli 2013)

Art. 28³⁰

II. Gegen
Verletzungen
1. Grundsatz

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

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

vom 10. Dezember 1907 (Stand am 1. Juli 2013)

Art. 28a³¹

2. Klage
a. Im
Allgemeinen³²

¹ Der Kläger kann dem Gericht beantragen:

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

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

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



Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

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 Bundesverfassung¹,
nach Einsicht in die Botschaft des Bundesrates vom 15. September 2017²,
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.



Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 2 Persönlicher und sachlicher Geltungsbereich

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

a. private Personen;

b. Bundesorgane.

Unternehmen sind auch private Personen

Kantone erlassen 26 Kantons-DSG

² Es ist nicht anwendbar auf:

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

Streichung: Schutz der Daten
juristischer Personen

natürlicher Personen

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 2020¹ (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:

Verordnung über Datenschutzzertifizierungen (VDSZ)

vom 31. August 2022

Der Schweizerische Bundesrat,

gestützt auf Artikel 13 Absatz 2 des Datenschutzgesetzes vom 25. September 2020¹ (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 1996² (AkkBV), soweit die vorliegende Verordnung keine abweichenden Vorschriften enthält.

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



Zulässigkeit der Bearbeitung von Personendaten

Informationspflicht

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.

- Gesetzliche Grundlage
- Ausdrückliche Einwilligung
- Überwiegendes öffentliches Interesse
- Überwiegendes privates Interesse -> Abschluss oder Abwicklung Vertrag

Verantwortlicher

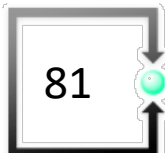
Verantwortlicher

Art. 4 § 7 DSGVO / Art. 5 Lit. j nDSG

- **Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
 - die allein oder gemeinsam mit anderen
 - über die **Zwecke und Mittel der Verarbeitung**
 - von personenbezogenen Daten
 - **entscheidet.**

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

Auftragsverarbeiter



Auftragsverarbeiter

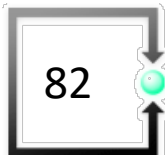
Art. 4 § 8 DSGVO / Art. 5 Lit. k und Art. 9 nDSG

- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle,
 - welche die personenbezogenen Daten
 - im Auftrag des Verantwortlichen
 - verarbeitet.

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

Er kommt in eine neue umfassende Mitverantwortung im Rahmen des Datenschutzes

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



Art. 28 (1) DSGVO / 9 nDSG

Zusammenarbeit mit Auftragsverarbeiter

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

so arbeitet dieser nur mit **Auftragsverarbeitern** zusammen,

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

Alle Verträge mit Auftragsverarbeitern müssen überprüft und allenfalls angepasst werden.

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

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

Zusammenarbeit mit Auftragsverarbeiter

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

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

Art. 28 (4) DSGVO / 9 nDSG

Zusammenarbeit mit Auftragsverarbeiter - Drittbeizug

Zieht der Auftragsverarbeiter seinerseits

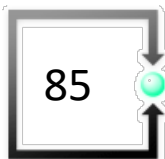
Dritte für die Verarbeitung

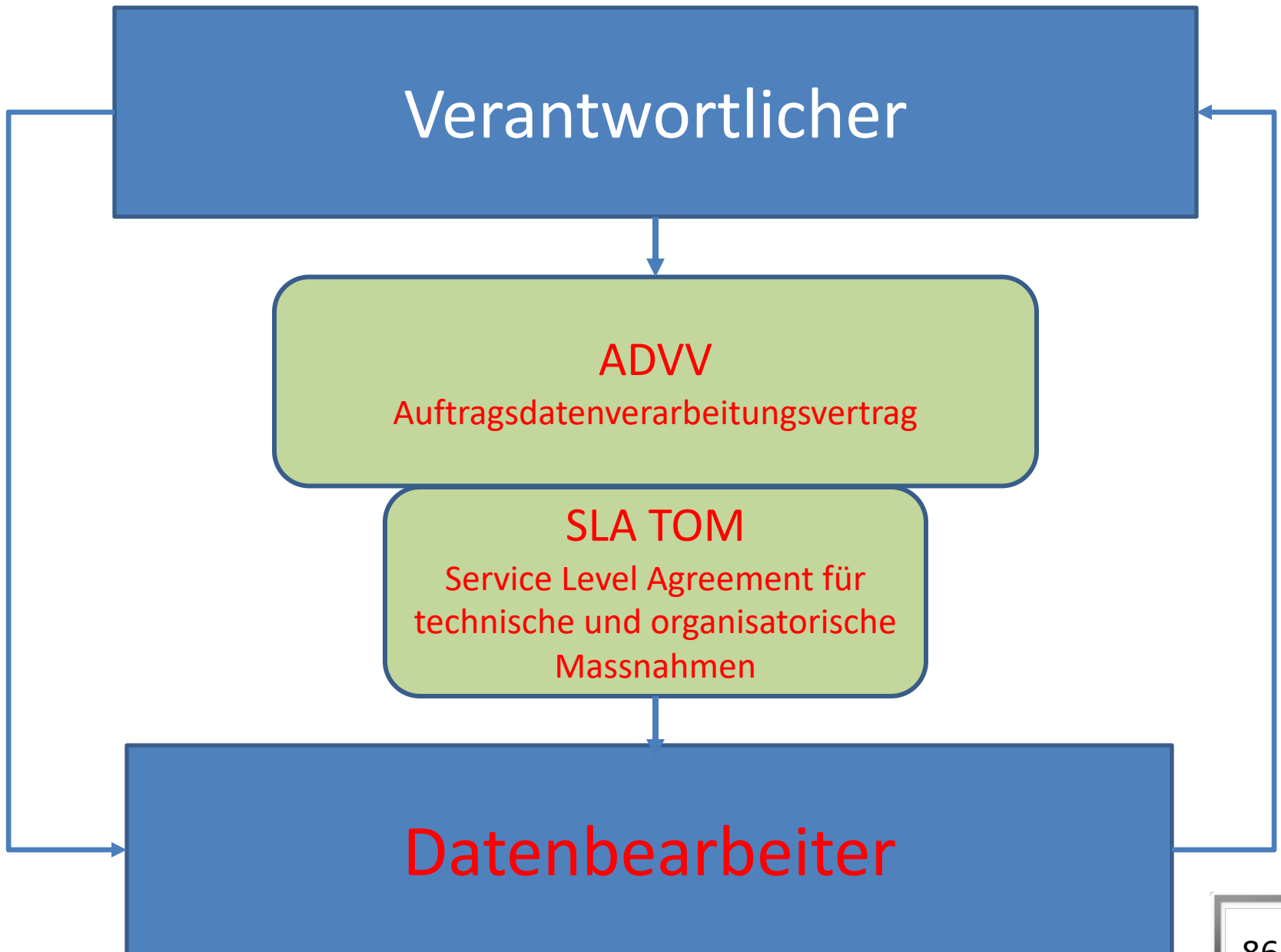
von personenbezogenen Daten bei, muss er diesem

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

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

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





Meldepflichten

Data Breach Notifications (DSGVO)

§ 33 DSGVO und Art. 24 nDSG



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.

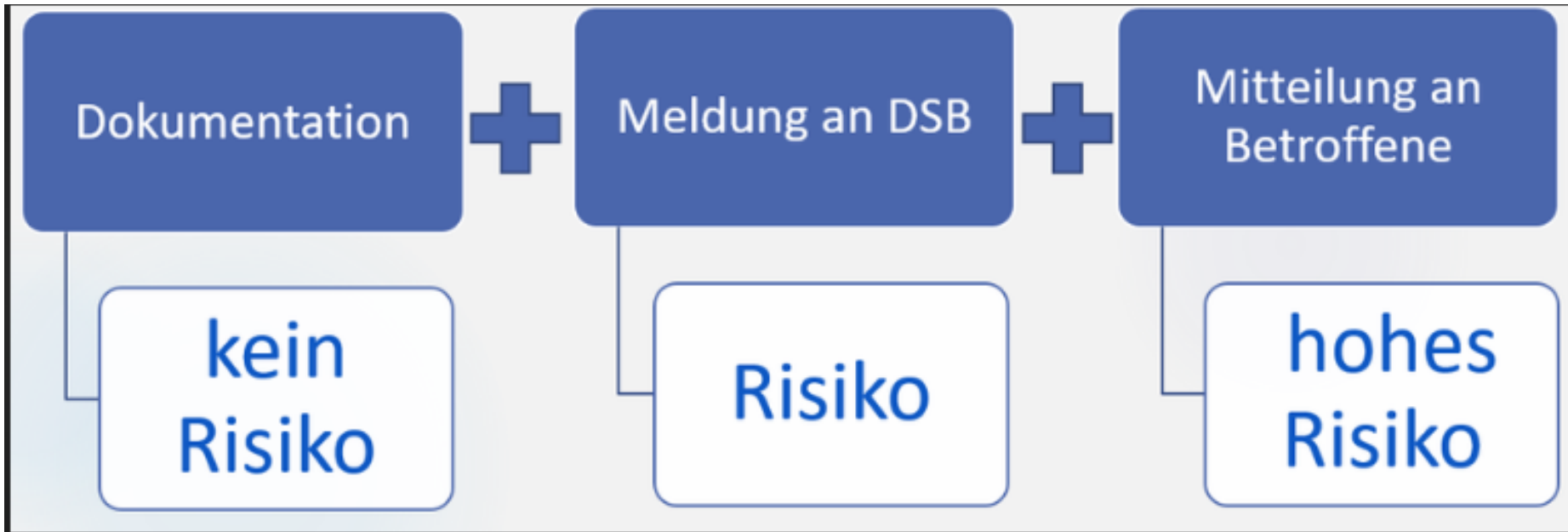
Benachrichtigung an Betroffene

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



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.

² In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

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

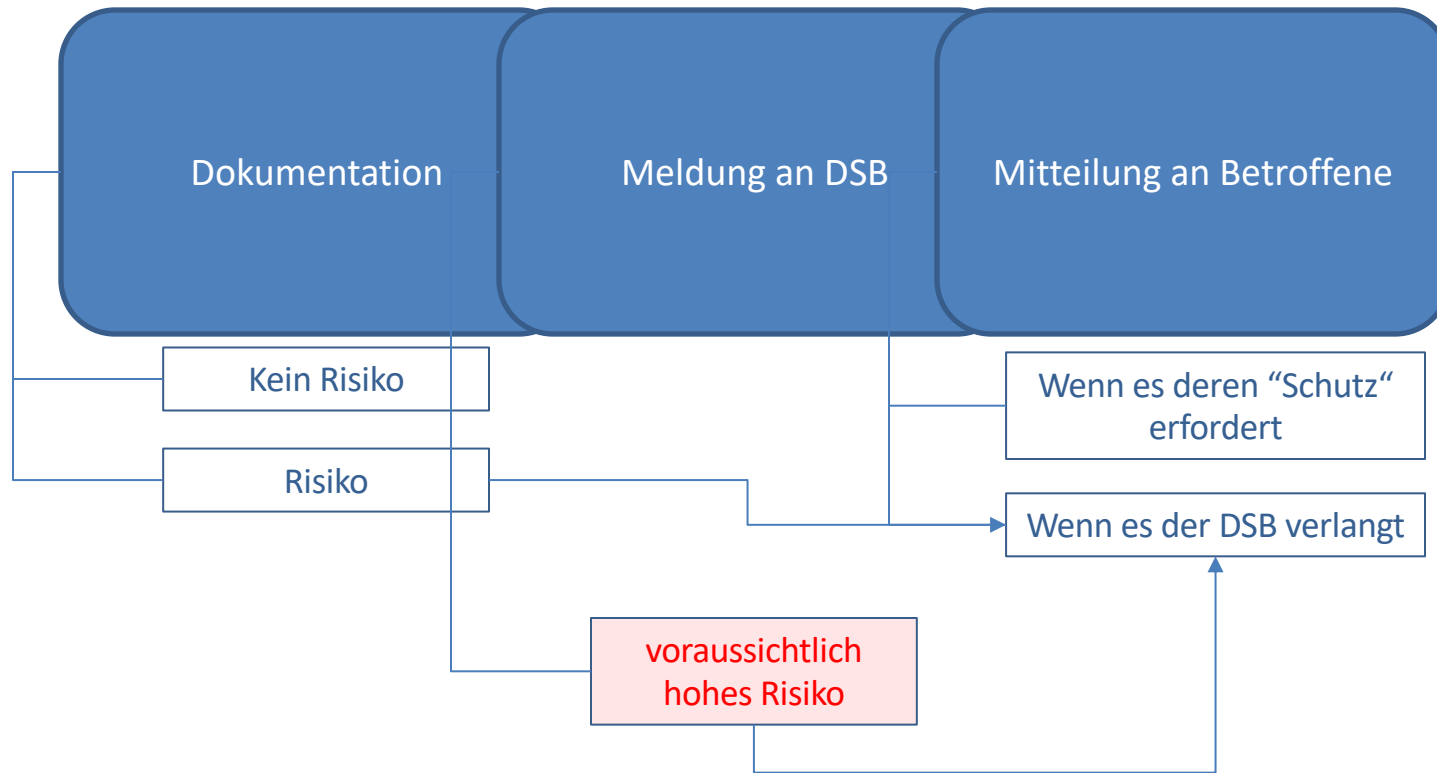
⁴ **Der Verantwortliche** informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.

⁵ Er kann die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn:

- a. ein Grund nach Artikel 26 Absatz 1 Buchstabe b oder Absatz 2 Buchstabe b vorliegt oder eine gesetzliche Geheimhaltungspflicht dies verbietet;
- b. die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert; oder
- c. die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.

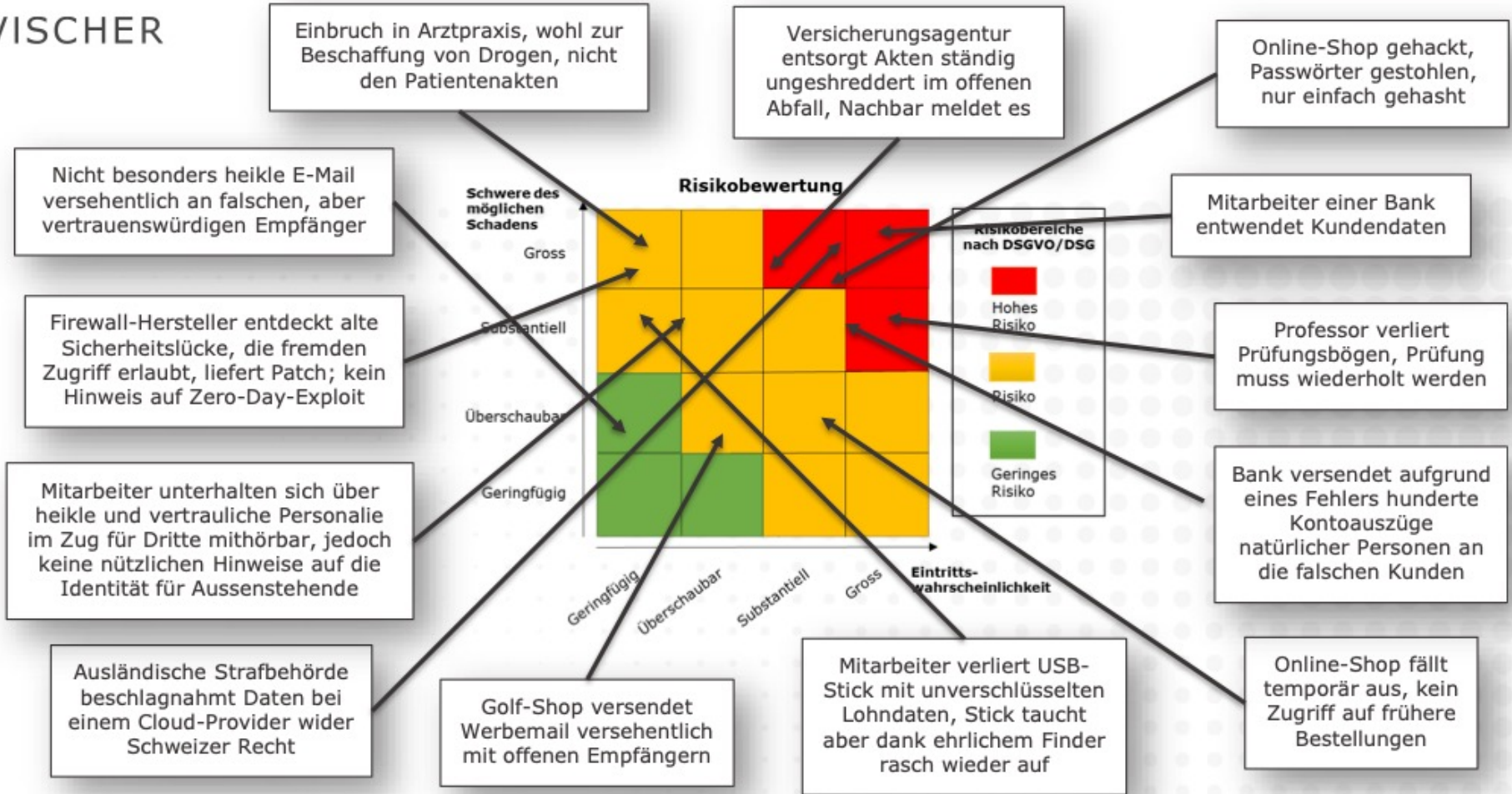
⁶ Eine Meldung, die aufgrund dieses Artikels erfolgt, darf in einem Strafverfahren gegen die meldepflichtige Person nur mit deren Einverständnis verwendet werden.

Meldung und Benachrichtigung nach nDSG



Beurteilung der Risikosituation

VISCHER



Grundsätze der IT-Sicherheit im neuen Datenschutzrecht

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;

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

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

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



Ablauf der Referendumsfrist: 14. Januar 2021

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

vom 25. September 2020

Art. 8 **Datensicherheit**

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

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

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

Datenbearbeitungsvertrag mit Auftragsbearbeiter (ADV)

Vertrags- und Auditpflichten für
Verantwortlichen

Art. 9 Bearbeitung durch Auftragsbearbeiter

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

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

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

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

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

vom ...

Schutzziele

Art. 2 Schutzziele

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

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

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

vom ...

Schutzziele



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



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

https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/km2024/23012024_leitfaden_tom.html

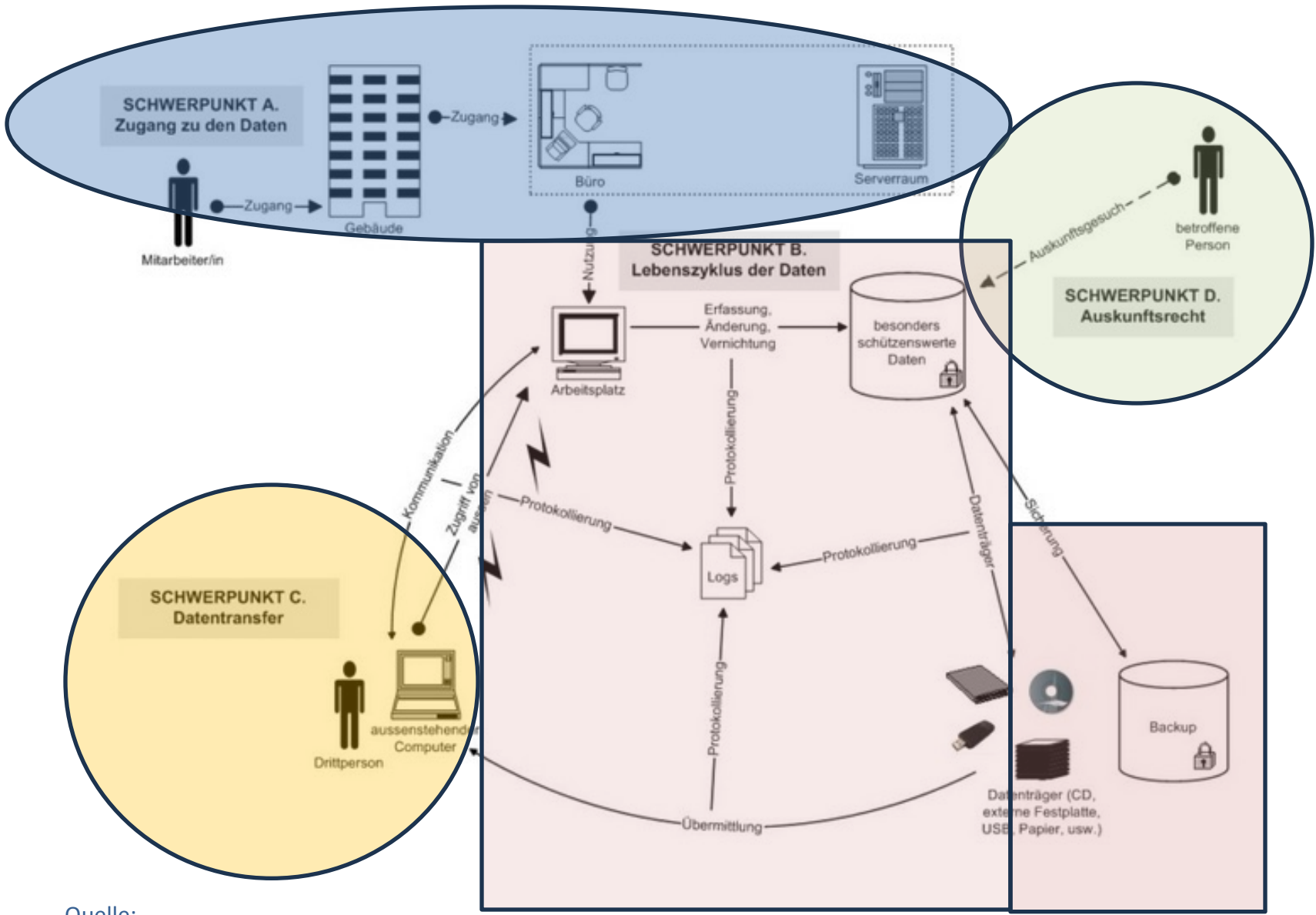
15. Januar 2024

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

15. Januar 2024

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

INHALTSVERZEICHNIS	
1	Einleitung 4
1.1	Datenschutzgesetz 4
1.2	Begriffe 5
1.3	Allgemeine Grundsätze 6
1.4	Funktionen 7
1.5	Technische und organisatorische Massnahmen 7
1.6	Hilfsmittel 7
2	Datenbearbeitung 9
2.1	Datenschutz-Folgenabschätzung 9
2.1.1	Pflicht zur Erstellung einer DSFA 10
2.1.2	Ausnahmen von der Pflicht zur Erstellung einer DSFA 10
2.1.3	Datenschutzberaterin oder Datenschutzberater 10
2.1.4	Bestandteile einer DSFA 11
2.2	Verzeichnis 11
2.3	Meldung von Verletzungen 12
2.4	Verantwortliche im Ausland 13
3	Rechte und Pflichten 15
3.1	Informationspflicht 15
3.2	Rechte der betroffenen Personen 16
3.2.1	Auskunftsrecht 17
3.2.2	Recht auf Datenherausgabe oder -übertragung 18
3.2.3	Recht auf Vernichtung der Personendaten 19
3.2.4	Recht auf Berichtigung der Personendaten 19
3.2.5	Recht auf Verbot der Bearbeitung von Personendaten 19
3.2.6	Recht auf Verbot der Bekanntgabe von Personendaten 20
3.2.7	Recht auf Mitteilung der Massnahmen betreffend Personendaten 20
3.3	Reproduzierbarkeit der Verfahren 20
4	Bundesorgane 22
4.1	Gesetzliche Grundlagen 22
4.2	Datenbearbeitung für nicht personenbezogene Zwecke 22
4.3	Bekanntgabe 23
4.4	Verzeichnis der Datenbearbeitungen 23
4.5	Meldung von Verletzungen der Datensicherheit 23
4.6	Automatisierte Einzelentscheidungen 23
4.7	Informationspflicht 24
4.8	Rechte der betroffenen Personen 24
4.9	Protokollierung 24
4.10	Bearbeitungsreglement 24
5	Datenschutz 26
5.1	Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen 26
5.2	Pseudonymisierung 27
5.3	Anonymisierung 28
5.4	Generalisierung 30
5.5	Minimierung 31
5.6	Randomisierung 31
5.7	Homomorphe Verschlüsselung 32
5.8	Synthetische Daten 32
6	Infrastruktur 33
6.1	Sicherheit der Räumlichkeiten 33
6.2	Sicherheit der Serverräume 34
6.3	Sicherheit der Arbeitsplätze 34
6.4	Cloud-Nutzung 35
6.5	Zur Vertiefung 36
7	Zugriff und Bearbeitungen 37
7.1	Zugriffsverwaltung 37
7.2	Identifizierung und Authentifizierung 37
7.3	Zugang zu den Daten 38
7.4	Zugang von ausserhalb der Organisation 39
7.5	Zur Vertiefung 39
8	Lebenszyklus der Daten 40
8.1	Datenerfassung 40
8.2	Verschlüsselung 41
8.3	Sicherheit der Datenträger 42
8.4	Datensicherung 42
8.5	Datenvernichtung 43
8.6	Sicherheits- und Schutzstufe 43
8.7	Protokollierung 45
8.8	Bearbeitungsreglement 46
9	Datenaustausch und -übermittlung 48
9.1	Netzsicherheit 48
9.2	Verschlüsselung von Mitteilungen 49
9.3	Digital Unterzeichnen von Mitteilungen (signieren) 50
9.4	Übergabe von Datenträgern 51
9.5	Protokollierung des Datenaustauschs 52
9.6	Datenbekanntgabe ins Ausland 52
9.7	Bearbeitung durch Auftragsbearbeiter 53
10	Schlussbemerkungen 54
11	Referenzen 55



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 <u>konkrete</u> Sicherheitsvorgaben, welche dieser umzusetzen und einzuhalten hat? Wenn ja, welche? Kann er dafür die entsprechenden Vorgaben vorlegen?		
5.2. Wie stellt der Anbieter <u>konkret</u> 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 <u>konkret</u> anwendet (Ziffer 6.4 Rahmenvertrag)?		
5.4. Wie stellt der Anbieter <u>konkret</u> sicher, dass nur berechnigte Personen auf die		

20 Massnahmenvorschläge

Datenschutzbeauftragter (DSGVO) Datenschutzberater (nDSG)

vom 25. September 2020

Art. 10 Datenschutzberaterin oder -berater

1 Private Verantwortliche **können** eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

2 Die Datenschutzberaterin oder der **Datenschutzberater** ist Anlaufstelle für die betroffenen Personen und für die Behörden, die in der Schweiz für den Datenschutz zuständig sind. Sie oder er hat namentlich folgende Aufgaben:

- a. Schulung und Beratung des privaten Verantwortlichen in Fragen des Datenschutzes;
- b. Mitwirkung bei der Anwendung der Datenschutzvorschriften.

3 Private Verantwortliche können von der Ausnahme nach Artikel 23 Absatz 4 Gebrauch machen, wenn die folgenden Voraussetzungen erfüllt sind:

- a. Die Datenschutzberaterin oder der **Datenschutzberater** übt ihre oder seine Funktion gegenüber dem Verantwortlichen fachlich unabhängig und weisungsungebunden aus.

4 Der private Verantwortliche kann von der Konsultation des EDÖB absehen, wenn er die Datenschutzberaterin oder den Datenschutzberater nach Artikel 10 konsultiert hat.

- b. Sie oder er übt keine Tätigkeiten aus, die mit ihren oder seinen Aufgaben als Datenschutzberaterin oder -berater unvereinbar sind.
- c. Sie oder er verfügt über die erforderlichen Fachkenntnisse.
- d. Der Verantwortliche veröffentlicht die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters und teilt diese dem EDÖB mit.

⁴ Der Bundesrat regelt die Ernennung von Datenschutzberaterinnen und Datenschutzberatern durch die Bundesorgane.

Benennung eines Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter **benennen auf jeden Fall** einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung** von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht.

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

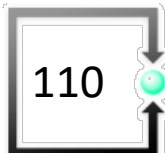
(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Passende Erwägungsgründe

(97) Datenschutzbeauftragter

Cloud-Computing und Auslandsspeicherung



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 keine Entscheidung 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, ausstellt 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

I. 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.

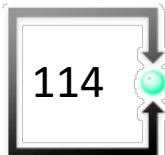
Namhafte Softwarehersteller wie Microsoft, Google, Amazon und

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.





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:

- 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
- 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
- Restrisikobeurteilung (Abwägung)



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 Schweiz vorgenommen werden. Wenn aber Daten ins Ausland



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

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

27. August 2021

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.

Datenschutzverordnung

235.11

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***

- * Die Beurteilung der Angemessenheit des Datenschutzes schliesst die Bekanntgabe von Personendaten nach der Richtlinie (EU) 2016/680⁷ 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.

- 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**



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

Beilage in den Unterlagen

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

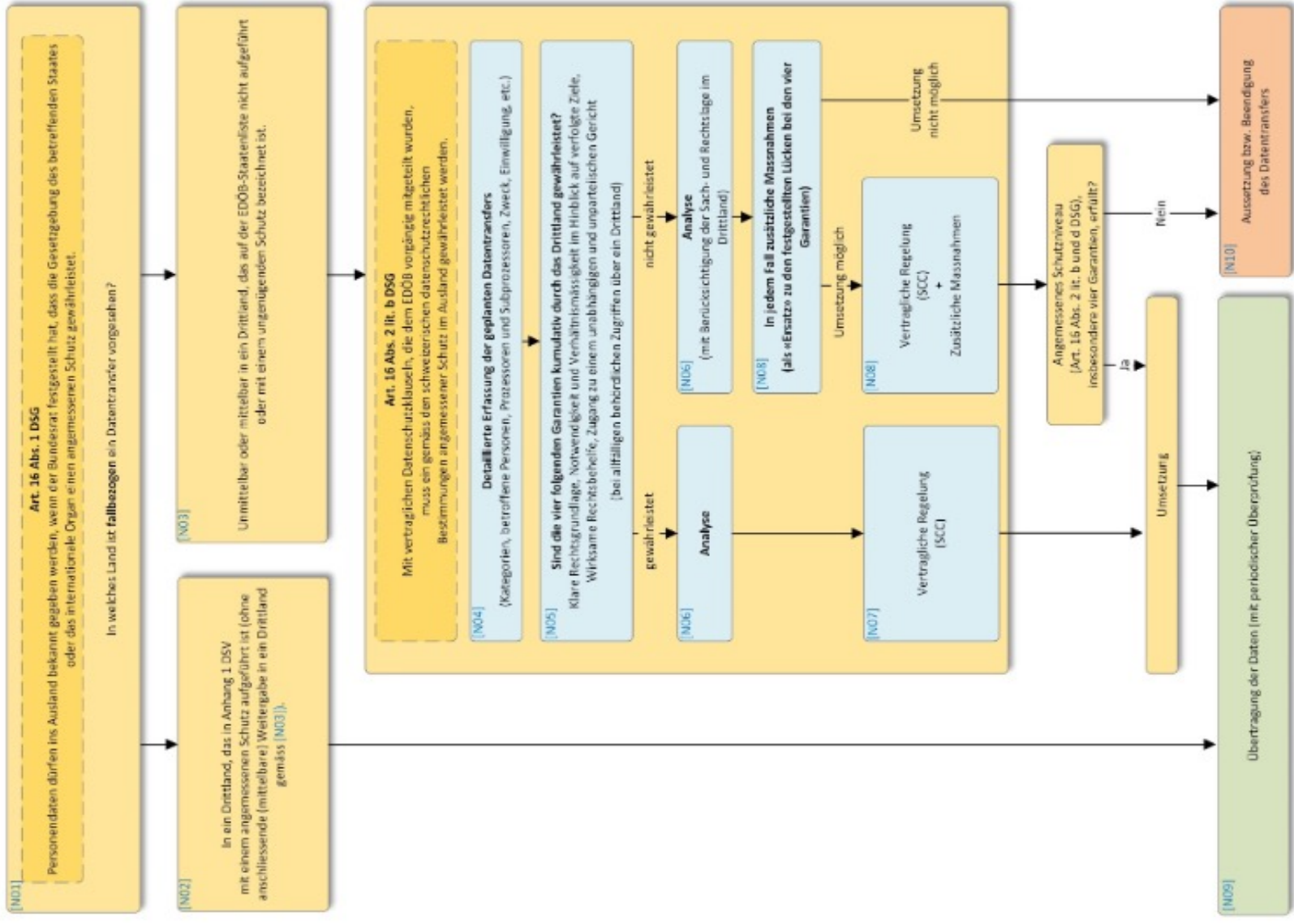
MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Datenexporteur(e): *[Name und Kontaktdaten des Datenexporteurs/der Datenexporteure und gegebenenfalls seines/ihrer 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.
Datenimporteuer(e): *[Name und Kontaktdaten des Datenexporteurs/der Datenimporteure, einschließlich jeder für den Datenschutz zuständigen Kontaktperson]*

1. Name:
Anschrift:





MARCH 25, 2022

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

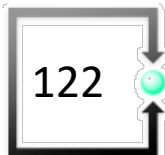


[BRIEFING ROOM](#)

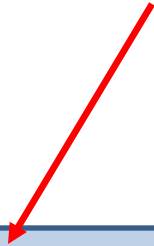
[STATEMENTS AND RELEASES](#)

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



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 tiefgehend und wird dann entscheiden, ob es zu einer Entscheidung Schrems III kommen wird.

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.

Sanktionen der DSGVO

Sanktionen

Aufsichtsbehörden in EU-Ländern

- **Direktes Sanktionierungsrecht der staatliche Datenschutzaufsichtsbehörden** gegenüber Unternehmen
- 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

In seiner Sitzung von 24.5.2023 hat der **Europäische Datenschutzausschuss (EDSA,** engl. **European Data Protection Board, EDPB)** die **Leitlinien 04/2022 zur Bußgeldzumessung nach der DSGVO** nach einer öffentlichen Konsultation angenommen ([🔗 Guidelines 04/2022 on the calculation of administrative fines under the GDPR](#)).

https://edpb.europa.eu/system/files/2023-06/edpb_guidelines_042022_calculationofadministrativefines_en.pdf

Guidelines



Guidelines 04/2022 on the calculation of administrative fines under the GDPR

Version 2.1

Adopted on 24 May 2023

Adopted

Table of Contents

EXECUTIVE SUMMARY	3
CHAPTER 1 – INTRODUCTION	6
1.1 - Legal framework.....	6
1.2 - Objective.....	7
1.3 - Scope.....	7
1.4 - Applicability.....	8
CHAPTER 2 – METHODOLOGY FOR CALCULATING THE AMOUNT OF THE FINE	8
2.1 - General considerations.....	8
2.2 - Overview of the methodology.....	9
2.3 - Infringements with fixed amounts.....	9
CHAPTER 3 – CONCURRENT INFRINGEMENTS AND THE APPLICATION OF ARTICLE 83(3) GDPR	9
Diagram	11
3.1 - One sanctionable conduct.....	12
3.1.1 - Concurrence of Offences.....	13
3.1.2 - Unity of action - Article 83(3) GDPR.....	15
3.2 - Multiple sanctionable conducts.....	16
CHAPTER 4 – STARTING POINT FOR CALCULATION	17
4.1 - Categorisation of infringements under Articles 83(4)–(6) GDPR.....	17
4.2 - Seriousness of the infringement in each individual case.....	17
4.2.1 - Nature, gravity and duration of the infringement.....	18
4.2.2 - Intentional or negligent character of the infringement.....	19
4.2.3 - Categories of personal data affected.....	20
4.2.4 - Classifying the seriousness of the infringement and identifying the appropriate starting amount.....	21
4.3 - Turnover of the undertaking with a view to imposing an effective, dissuasive and proportionate fine.....	23
CHAPTER 5 – AGGRAVATING AND MITIGATING CIRCUMSTANCES	26
5.1 - Identification of aggravating and mitigating factors.....	26
5.2 - Actions taken by controller or processor to mitigate damage suffered by data subjects.....	26
5.3 - Degree of responsibility of the controller or processor.....	27
5.4 - Previous infringements by the controller or processor.....	27
5.4.1 - Time frame.....	28
5.4.2 - Subject matter.....	28
5.4.3 - Other considerations.....	28
5.5 - Degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement.....	29
5.6 - The manner in which the infringement became known to the supervisory authority.....	29
5.7 - Compliance with measures previously ordered with regard to the same subject matter.....	30
5.8 - Adherence to approved codes of conduct or approved certification mechanisms.....	30
5.9 - Other aggravating and mitigating circumstances.....	31
CHAPTER 6 – LEGAL MAXIMUM AND CORPORATE LIABILITY	34
6.1 - Determining the Legal Maximum.....	34
6.1.1 - Static maximum amounts.....	34
6.1.2 - Dynamic maximum amounts.....	34
6.2 - Determining the undertaking's turnover and corporate liability.....	35
6.2.1 - Determining an undertaking and corporate liability.....	35
6.2.2 - Determining the turnover.....	38
CHAPTER 7 – EFFECTIVENESS, PROPORTIONALITY AND DISSUASIVENESS	39
7.1 - Effectiveness.....	39
7.2 - Proportionality.....	39
7.3 - Dissuasiveness.....	41
CHAPTER 8 – FLEXIBILITY AND REGULAR EVALUATION	41
ANNEX – TABLE FOR ILLUSTRATION OF THE GUIDELINES 04/2022 ON THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR	43

Sanktionen nach schweizerischem Datenschutzrecht



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

vom 25. September 2020

8. Kapitel: Strafbestimmungen

Art. 60

Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

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

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

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



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.



Ablauf der Referendumsfrist: 14. Januar 2021

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

vom 25. September 2020

Art. 62 Verletzung der beruflichen Schweigepflicht

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

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

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



Ablauf der Referendumsfrist: 14. Januar 2021

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

vom 25. September 2020

Art. 63 Missachten von Verfügungen

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



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.

Die wichtigsten datenschutz- und datensicherheitsrechtlichen Aspekte für Unternehmen

Handlungsbedarf unter neuem CH-DSG

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



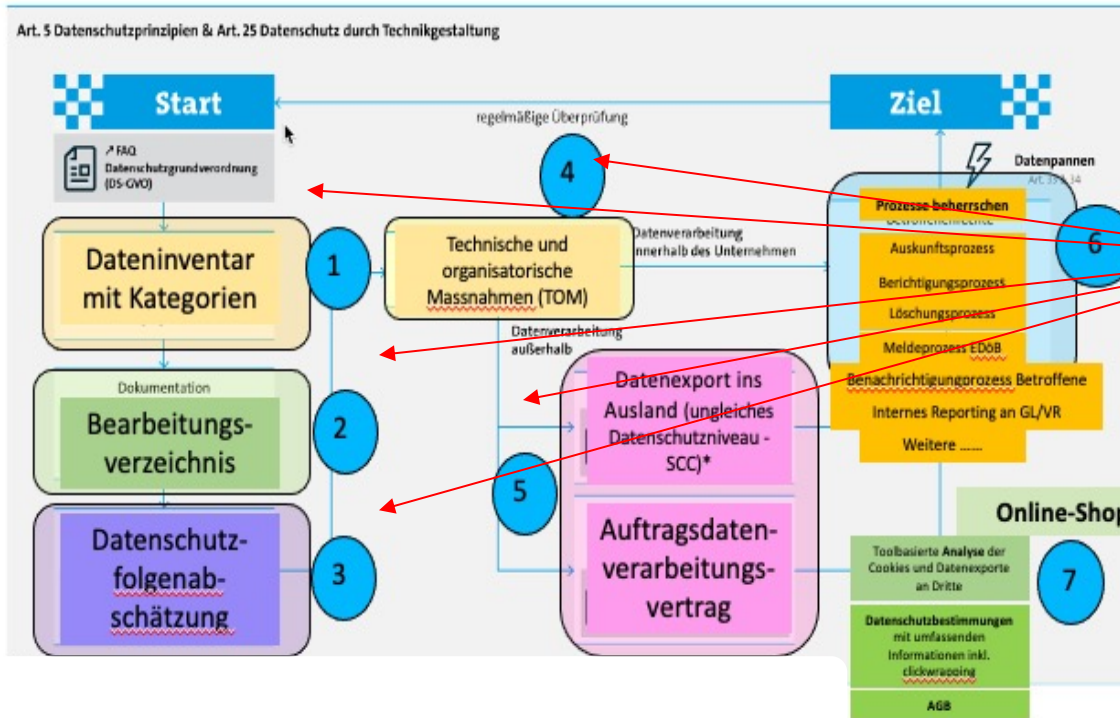
Handlungsbedarf unter neuem CH-DSG

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

Das Projektvorgehen



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

Xplain-Fall

Schlussbericht des EDÖB



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
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 vorgearbeitet. 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 Wartungsprozesse 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



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:

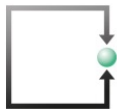
- Xplain hat 30 Tage Zeit zu erklären, ob sie die Empfehlungen des EDÖB akzeptiert und umsetzt.
- Lehnt sie ab, kann der EDÖB eine Verfügung erlassen, die dann ans Bundesverwaltungsgericht weitergezogen werden könnte.

Unterlagen für die Praxis



ANFORDERUNGEN AN CLOUD-SERVICE-PROVIDER

ZERTIFIZIERUNGEN VON DATENSCHUTZ-KONFORMITÄT NACH ISO 27001 UND NEU NACH ISO 27701 UND ISO 27018



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

Publikationen

Filter einblenden

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

Der Cloud-Standard ISO 27018 enthält für Anbieter von Cloud-Diensten spezifische datenschutzrechtliche Anforderungen. Er bietet Überwachungsmechanismen und Richtlinien für die Implementierung von Massnahmen zum Schutz personenbezogener Daten in der Cloud. Es werden speziell datenschutzrechtliche Anforderungen aus anderen Bereichen auf Informationssicherheitsrisiken im Bereich Cloud Computing angepasst. Der Standard ISO 27701 ist im Juli 2019 hinzugekommen. Dieser erweitert das ISMS nach ISO 27001 um datenschutzrechtliche Aspekte
Autor: RA Lukas Fässler, MLaw Milica Stefanovic

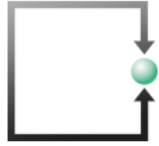
Anforderungen an Cloud-Service-Provider - Zertifizierungen von Datenschutzkonformität nach ISO 27001 und neu nach ISO 27701 und ISO 27018

Jetzt anrufen
oder E-Mail

Jetzt online
Konferenz

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



Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

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

Impressum Datenschutzbestimmungen

Profil Kompetenzen - Team Aktuell Publikationen Referenzen Kontakt

Aktuelles aus unserer Kanzlei.

Alle Intern Publikationen Veranstaltungen

CAS Information-Security und Risk-Management

Verfasst am 29.05.2019

Fachhochschule Nordwest-Schweiz, FHNW in Basel

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

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

Datenschutz und Datensicherheit in der Arztpraxis

Verfasst am 16.05.2019

Jetzt anrufen 041 727 60 80
oder E-Mail schreiben

FSDZ Rechtsanwälte & Notariat AG

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

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

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

Fragen

Aufgabe 1

Formulieren Sie eine Data Protection and Security Policy des Verwaltungsrates an die Unternehmensleitung und die Mitarbeitenden.

(max. 3 Grundsätze, was dem VR in Bezug auf die Einhaltung der Datenschutz- und Datensicherheitsanforderungen wichtig ist).

Aufgabe 2

Die Firma XY AG wird eine neue Palette von Cloudservices bei der Cloud AG beziehen:

- Infrastructure as a Service (IaaS)
- Backup as a Service (BaaS)
- Filesharing as a Service (FaaS)

Im FaaS wird die XY AG u.a. auch Mitarbeiterdaten (Lohndaten, Sozialversicherungsdaten, Ferien- und Krankheitsabsenzen, vertrauensärztliche Atteste ihrer Mitarbeitenden) speichern.

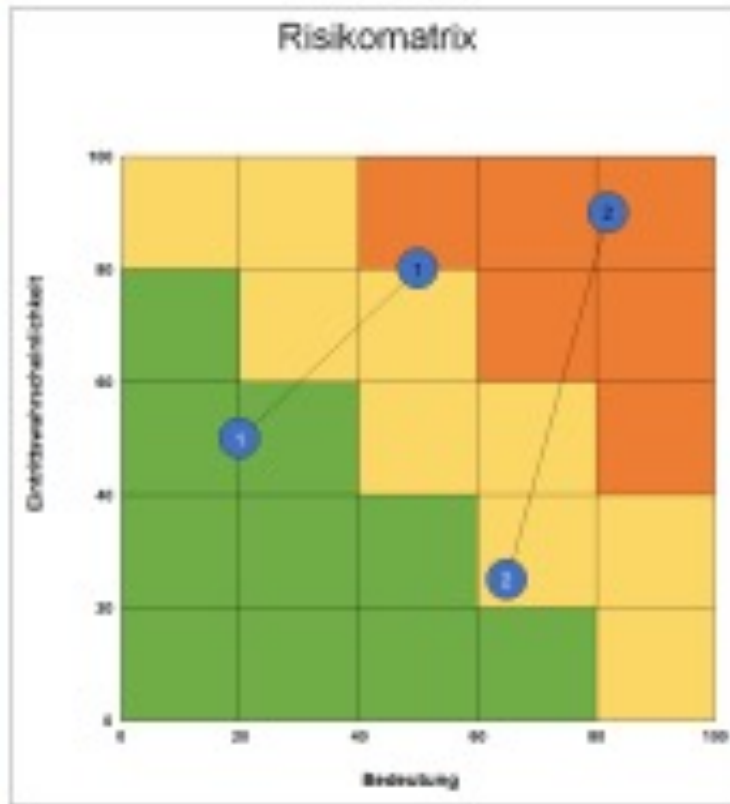
Erstellen Sie für die XY AG eine Datenschutz-Folgeabschätzung in Bezug auf diese ausgelagerten Personendaten

- Risikofaktoren für die personenbezogenen Daten (R1 bis Rx)
- Schadenshöhe pro Risikofaktor
- Eintretenswahrscheinlichkeit pro Risikofaktor

Risikomatrix (5 x 5)



Risiko-Nr.	Beschreibung	W	W	W	W
1	Risiko 1	W	W	W	W
2	Risiko 1	W	W	W	W
3	Risiko 1				
4	Risiko 1				
5	Risiko 1				
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					



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

