CAS Cybersecurity und Information Risk Management

Rechtliche Aspekte

Lukas Fässler
Rechtsanwalt & Informatikexperte
FSDZ Rechtsanwälte & Notariat AG Zug
www.fsdz.ch faessler@fsdz.ch

Rechtsanwälte
ATTORNEYS @ LAW

FSDZ Rechtsanwälte & Notariat AG

www.fsdz.ch

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

Impressum Datenschutzbestimmungen

Profil Kompetenzen Team Aktuell Publikationen Referenzen Kontakt

Hinweis schliessen

Umsetzung der DSGVO

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

Jetzt anrufen 041 727 60 80
oder E-Mail schreiben

FSDZ Rechtsanwälte & Notariat AG

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

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

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

Assoziierte selbständige Anwältin:

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

Partnerkanzlei de la cruz beranek Rechtsanwälte AG, Zug

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

Lukas Fässler

Rechtsanwalt und Informatikexperte, Certified Software Asset Manager IAITAM Inc.

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

Profil

1975 – 1980
Studium an der Universität Fribourg/CH

1982
Anwaltspatent des Kantons Luzern

1982 – 1984
Gerichtsschreiber am Amtsgericht Hochdorf

1984 - 1987
Gerichtsschreiber am Verwaltungsgericht Luzern

1987 - 1992
EDV-Beauftragter im Gerichtswesen Kanton Luzern

1992 - 1997
Informatikchef des Kantons Luzern

1997
Selbständiger Spezialanwalt seit September 1997

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

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

Verwaltungsratsmandate

- Verwaltungsratspräsident 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


WARNING: NO TRESPASSING
COLONIAL PIPELINE
SOUTH BALTIMORE
DELIVERY

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

CYBERATTACKE

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)

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

News > Schweiz >

Cyberkriminalität

Hackerangriff auf die Gemeinde Montreux

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

Dieser Artikel wurde **4**-mal geteilt.

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

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

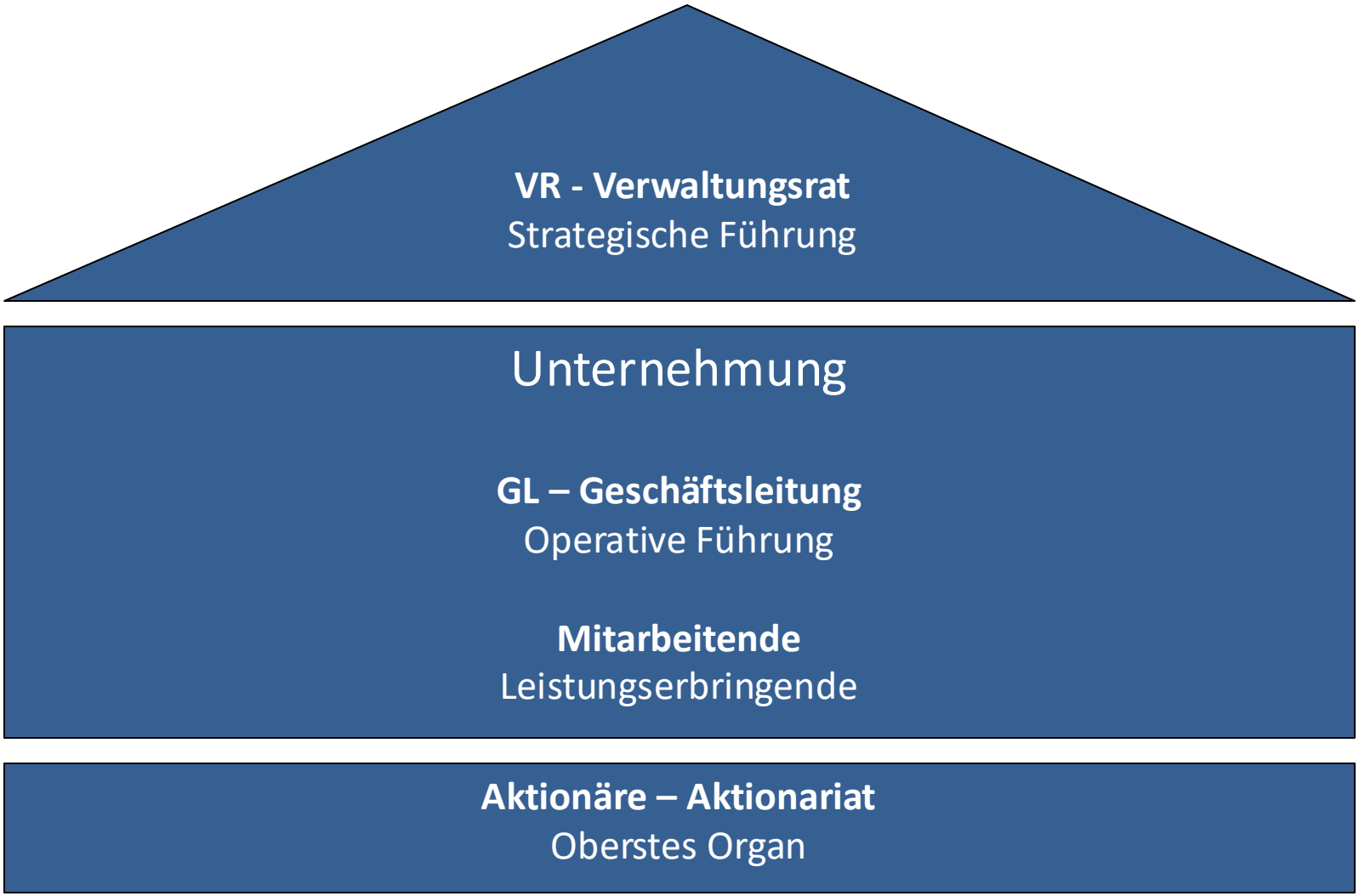
Seit der Ankündigung der Ukraine-Friedenskonferenz auf dem Bürgenstock ist die Zahl russischer Cyberangriffe rasant angestiegen.

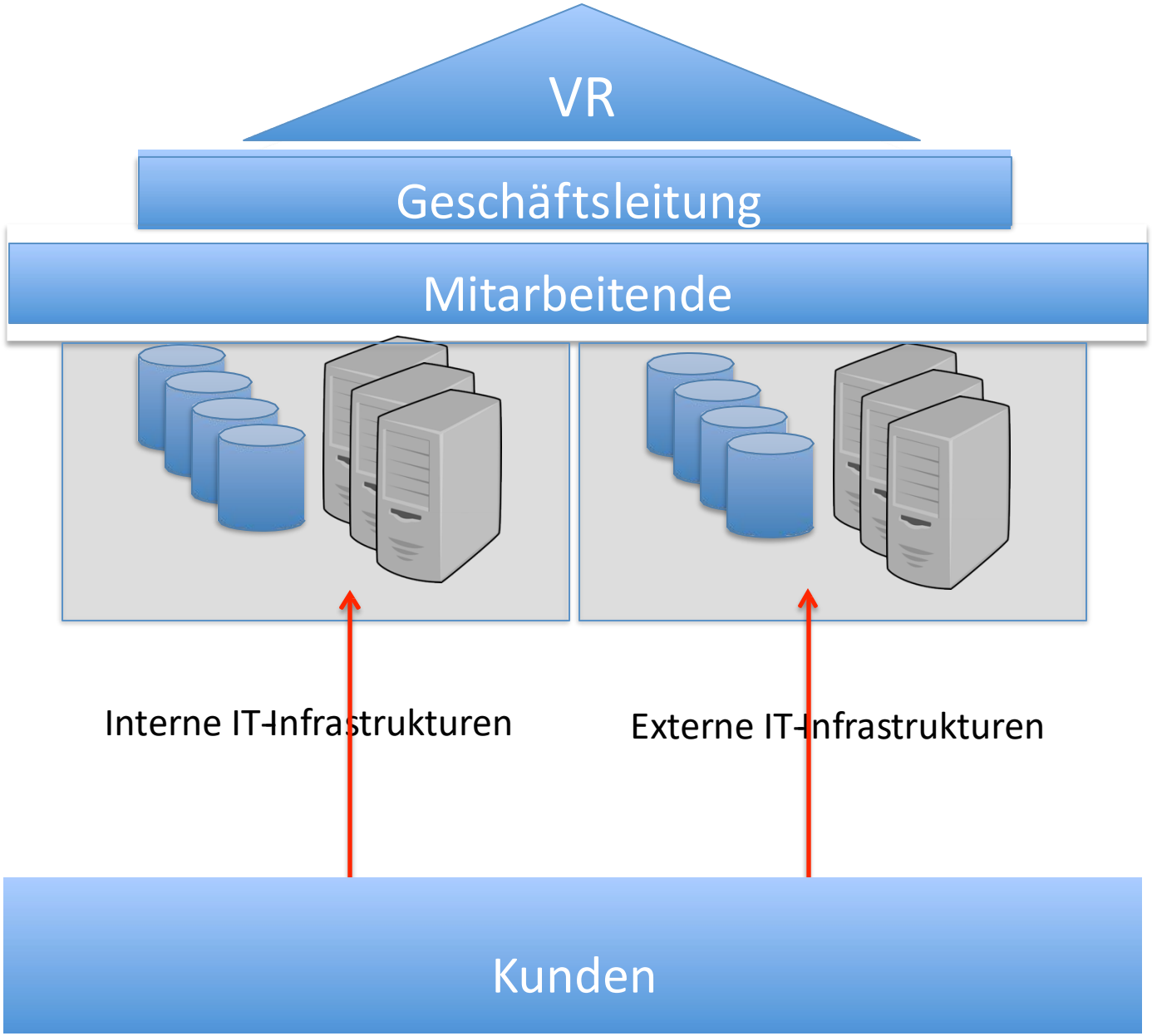
09.06.2024 08:13

Teil 1

Grundsätze der Unternehmensführung

Das Unternehmen

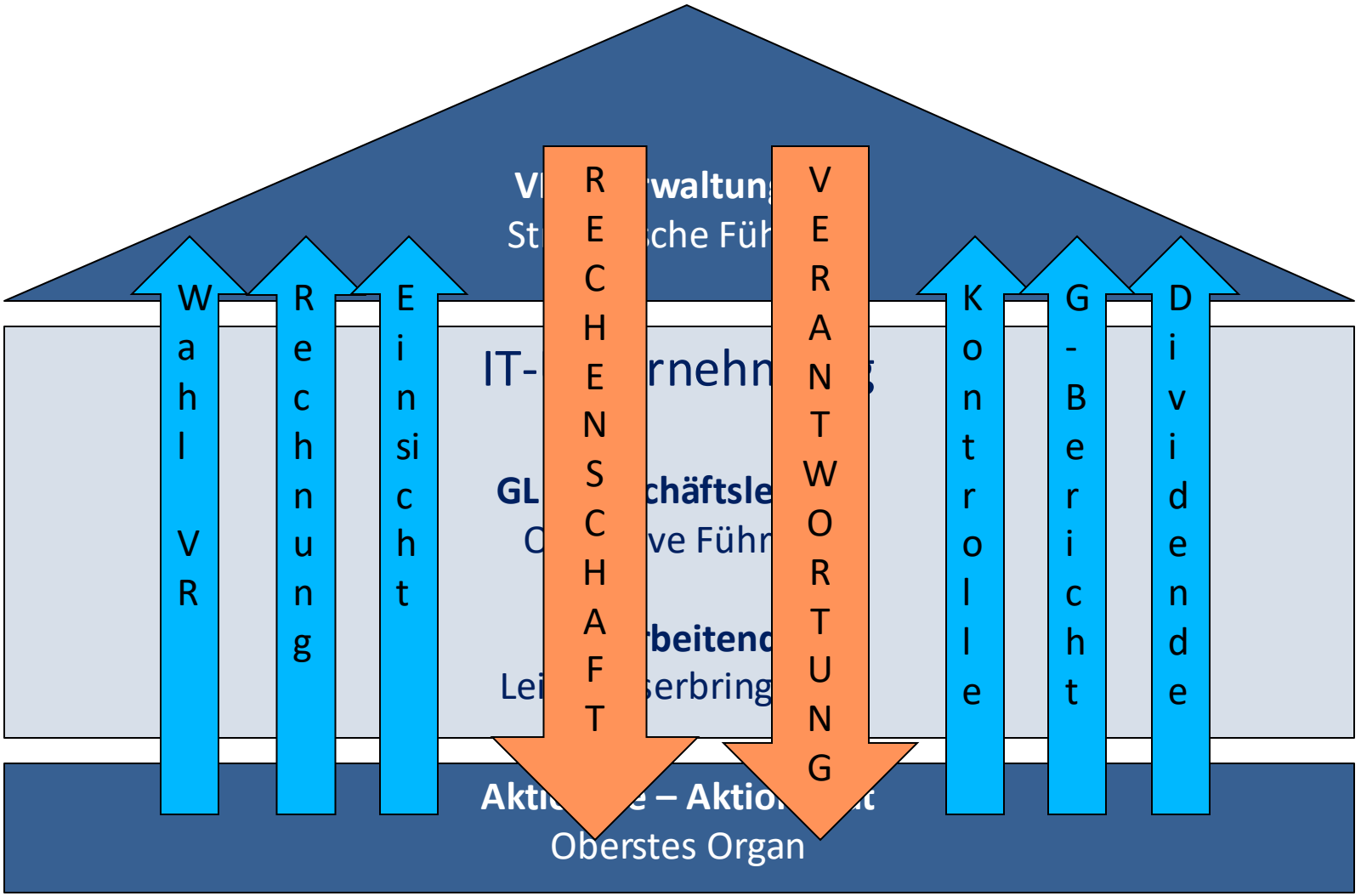

VR - Verwaltungsrat
Strategische Führung
Unternehmung
GL – Geschäftsleitung
Operative Führung
Mitarbeitende
Leistungserbringende
Aktionäre – Aktionariat
Oberstes Organ


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

Die gesetzlichen Grundlagen zur Unternehmensführung

Die Generalversammlung der Aktionäre

Aktionäre – Aktionariat
Oberstes Organ


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

Dritter Abschnitt: Organisation der Aktiengesellschaft

A. Die Generalversammlung

Art. 698

I. Befugnisse

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

[2] Ihr stehen folgende unübertragbare Befugnisse zu:

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

Aktionäre – Aktionariat
Oberstes Organ

Zweiter Abschnitt: Rechte und Pflichten der Aktionäre

Art. 660[324]

A. Recht auf Gewinn- und Liquidationsanteil

I. Im Allgemeinen

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

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

Aktionäre – Aktionariat
Oberstes Organ

Der Verwaltungsrat
Oberste strategische Führung

VR - Verwaltungsrat
Strategische Führung

Art. 716*a*[430]

2. Unübertragbare Aufgaben

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

1. die Oberleitung der Gesellschaft und die Erteilung der nötigen Weisungen;
2. die Festlegung der Organisation;
3. die Ausgestaltung des Rechnungswesens, der Finanzkontrolle sowie der Finanzplanung, sofern diese für die Führung der Gesellschaft notwendig ist;
4. die Ernennung und Abberufung der mit der Geschäftsführung und der Vertretung betrauten Personen;
5. die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen;
6. die Erstellung des Geschäftsberichtes[431] sowie die Vorbereitung der Generalversammlung und die Ausführung ihrer Beschlüsse;
7. die Benachrichtigung des Richters im Falle der Überschuldung.

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

B. Der Verwaltungsrat[414]

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

Compliance-Verantwortung

VR - Verwaltungsrat
Strategische Führung

B. Der Verwaltungsrat[414]

Art. 717[433]

IV. Sorgfalts- und Treuepflicht

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

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

Sorgfaltspflichten innerhalb öffentlicher Verwaltungen

Beispiel: Kanton Luzern

20

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

§ 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 der Regierungsrat die wichtigsten selbst. Die andern überträgt er den Departementen, der Staatskanzlei, den Dienstst 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, Geschäftsführung und Liquidation

Art. 754[488]

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

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

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

Urteilskopf

139 III 24

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

Regeste a

Art. 754 OR; aktienrechtliche Verantwortlichkeit.
Haftung des Verwaltungsrats für die Kosten eines erfolglos geführten Prozesses über die Eintragung von Namenaktien im Aktienbuch der Gesellschaft, in dem erkannt wurde, die Verweigerung der Eintragung sei nicht im Interesse der Gesellschaft erfolgt und habe gegen das Gleichbehandlungsgebot der Aktionäre sowie gegen das Rechtsmissbrauchsverbot verstossen (E. 3).

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

3.2 Nach **Art. 717 Abs. 1 OR** müssen die Mitglieder des Verwaltungsrats, sowie Dritte, die mit der Geschäftsführung befasst sind, ihre Aufgaben mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren. Die gesetzlich normierte Treuepflicht verlangt, dass die Mitglieder des Verwaltungsrats ihr Verhalten am Gesellschaftsinteresse ausrichten. Für die Sorgfalt, die der Verwaltungsrat bei der Führung der Geschäfte der Gesellschaft aufzuwenden hat, gilt ein objektiver Massstab. Die Verwaltungsräte sind zu aller Sorgfalt verpflichtet und nicht nur zur Vorsicht, die sie in eigenen Geschäften anzuwenden pflegen (**BGE 122 III 195** E. 3a S. 198; **BGE 113 II 52** E. 3a S. 56). Das Verhalten eines Verwaltungsratsmitglieds wird deshalb mit demjenigen verglichen, das billigerweise von einer abstrakt vorgestellten, ordnungsgemäss handelnden Person in einer vergleichbaren Situation erwartet werden kann (PETER BÖCKLI, Schweizer Aktienrecht, 4. Aufl. 2009, § 13 N. 575).

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

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

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

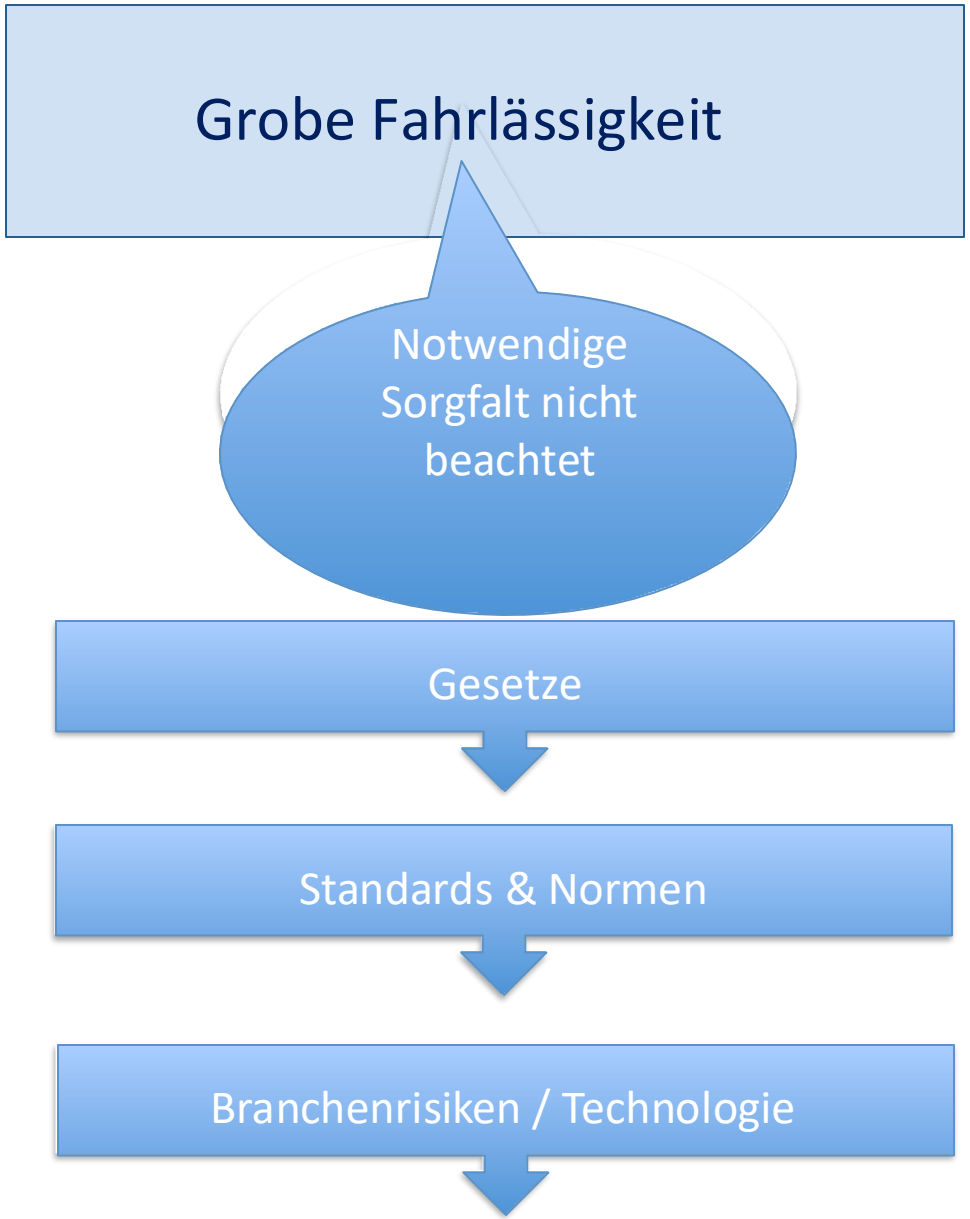
III. Haftung für Verwaltung, Geschäftsführung und Liquidation

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

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

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

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


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

Treuepflicht des Arbeitnehmers

II. Sorgfalts- und Treuepflicht

Art. 321*a*

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

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

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

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

Das BAG ist nicht verantwortlich – ist das wirklich so?

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

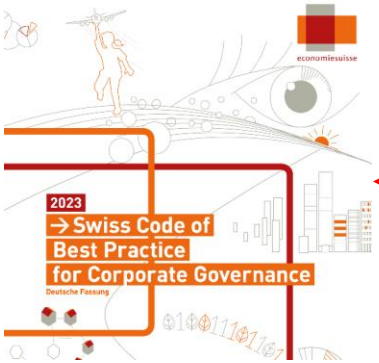
https://www.srf.ch/play/radio/echo-der-zeit/audio/datenschutzprobleme-bei-der-plattform-meineimfpungen-ch?id=fbbd88e3-0b77-4a1e-8c53-38cd4a92b443

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

Einfluss von Standards und Normen

Internes Kontrollsystem IKS

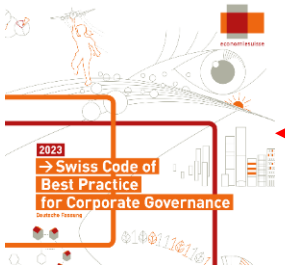
Im schweizerischen Obligationenrecht (OR) ist die Pflicht zur Führung eines internen Kontrollsystems (IKS) in Artikel 728a OR für Aktiengesellschaften verankert, die einer ordentlichen Revision unterliegen. Diese Vorschrift besagt, dass die Revisionsstelle im Rahmen ihrer Prüfung bestätigen muss, dass ein IKS existiert, und dass es den Geschäftsrisiken und der Tätigkeit des Unternehmens angepasst ist.



Internes Kontrollsystem IKS (2)

Der Kern der gesetzlichen Verpflichtung

- **Artikel 728a OR**: legt fest, dass die Revisionsstelle die Existenz eines internen Kontrollsystems zu prüfen hat.
- Dies betrifft nur Unternehmen, die zu einer ordentlichen Revision verpflichtet sind.
- Die Prüfung konzentriert sich auf die Existenz des IKS, also darauf, dass es dokumentiert, den Risiken angepasst und bekannt ist sowie tatsächlich angewendet wird.



Was das IKS leisten soll

- Das IKS dient dazu, die Zuverlässigkeit der Finanzberichterstattung sicherzustellen und Fehldarstellungen zu vermeiden.
- Es ist ein wesentlicher Beitrag zum Risikomanagement, da es Schwachstellen aufdeckt und eine wirksame, wiederkehrende Kontrolle ermöglicht.
- Das IKS soll einen Beitrag zur Sicherheit, Ordnungsmässigkeit und Wirtschaftlichkeit der Unternehmensprozesse leisten.

https://backend-api.economiesuisse.ch//sites/default/files/nn_migration/swisscode_d_web_1.pdf


economiesuisse
2023
→Swiss Code of Best Practice for Corporate Governance
Deutsche Fassung

Umgang mit Risiken, Compliance und Finanzüberwachung (internes Kontrollsystem)

26

Der Verwaltungsrat sorgt für ein dem Unternehmen angepasstes internes Kontrollsystem, welches Risikomanagement, Compliance und Finanzüberwachung umfasst.

- Das interne Kontrollsystem dient dem Ziel, die Effektivität und die Effizienz der Geschäftstätigkeit (Operations), die Gesetzes- und Normenkonformität (Compliance) sowie die Verlässlichkeit der finanziellen und nichtfinanziellen Berichterstattung (Reporting) sicherzustellen.
- Das operative Management und die es unterstützenden Funktionen sorgen dafür, dass die Kontrollen gemäss den Vorgaben des Verwaltungsrats umgesetzt werden und dass sie wirksam sind.
- Die Ausgestaltung des internen Kontrollsystems hat der Grösse, der Komplexität und dem Risikoprofil des Unternehmens Rechnung zu tragen.

Risikomanagement

27

Das Unternehmen verfügt über ein angemessenes Risikomanagement. Der Verwaltungsrat nimmt eine regelmässige Risikobeurteilung vor.

- Das Risikomanagement umfasst namentlich strategische, operationelle, rechtliche und finanzielle Risiken sowie Marktrisiken bzw. Risiken für die Reputation des Unternehmens.
- Der Verwaltungsrat nimmt mindestens einmal jährlich eine Risikobeurteilung vor und berücksichtigt deren Ergebnis für seine Leitungs- und Aufsichtsaufgaben sowie für die Weiterentwicklung des internen Kontrollsystems.

Compliance und verantwortungsvolles Handeln

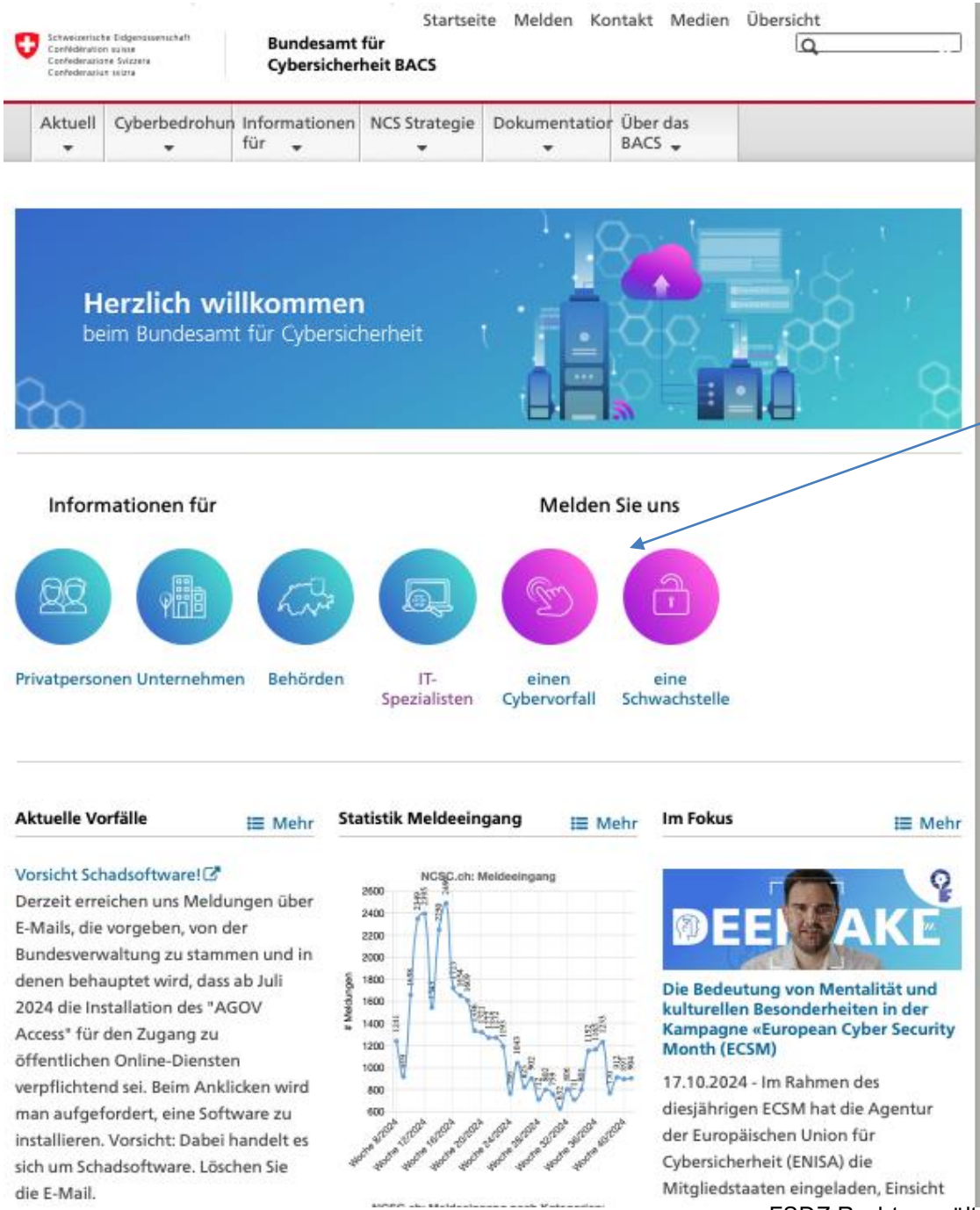
28

Der Verwaltungsrat ist dafür besorgt, dass das Unternehmen insgesamt Gesetze und interne Normen einhält (Compliance) und auch darüber hinaus verantwortungsvoll handelt.

- Der Verwaltungsrat ist im Rahmen seiner Oberaufsicht dafür besorgt, dass nicht nur seine Mitglieder, sondern das Unternehmen insgesamt, inklusive Management und Mitarbeitende, die Gesetze und internen Normen einhalten (Compliance) und dass auch darüber hinaus verantwortungsvoll gehandelt wird.
- Der Verwaltungsrat organisiert die Compliance nach den Besonderheiten des Unternehmens und erlässt geeignete Verhaltensrichtlinien. Er orientiert sich dabei an anerkannten Best-Practice-Regeln und beachtet die wichtige Rolle finanzieller wie nichtfinanzieller Anreize für Mitarbeitende und deren Vorgesetzte.[3]
- Die Geschäftsleitung trifft Massnahmen zur Einhaltung der Gesetze und internen Normen sowie für ein integres Geschäftsgebaren im Unternehmensalltag. Sie gewährt hierfür die erforderlichen personellen und finanziellen Ressourcen.

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

Branchen-Standards


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Bundesamt für Cybersicherheit BACS
Startseite Melden Kontakt Medien Übersicht
Aktuell
Cyberbedrohun
Informationen für
NCS Strategie
Dokumentatior
Über das BACS
Herzlich willkommen
beim Bundesamt für Cybersicherheit
Informationen für
Melden Sie uns
Privatpersonen
Unternehmen
Behörden
IT-Spezialisten
einen Cybervorfall
eine Schwachstelle
Aktuelle Vorfälle
Mehr
Vorsicht Schadsoftware!
Derzeit erreichen uns Meldungen über E-Mails, die vorgeben, von der Bundesverwaltung zu stammen und in denen behauptet wird, dass ab Juli 2024 die Installation des "AGOV Access" für den Zugang zu öffentlichen Online-Diensten verpflichtend sei. Beim Anklicken wird man aufgefordert, eine Software zu installieren. Vorsicht: Dabei handelt es sich um Schadsoftware. Löschen Sie die E-Mail.
Statistik Meldeeingang
Mehr
NCSC.ch: Meldeeingang
Meldungen
Im Fokus
Mehr
Die Bedeutung von Mentalität und kulturellen Besonderheiten in der Kampagne «European Cyber Security Month (ECSM)
17.10.2024 - Im Rahmen des diesjährigen ECSM hat die Agentur der Europäischen Union für Cybersicherheit (ENISA) die Mitgliedstaaten eingeladen, Einsicht

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.

Aktuell

SMIDEX SUISSE
Smart ID Exposyum

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

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

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 Schlüsselelement 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)

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)

Schweizerisches Strafgesetzbuch 311.0

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Art. 143

Unbefugte Daten beschaflhng

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

Schweizerisches Strafgesetzbuch **311.0**

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Art. 143bis

Unbefugtes Eindringen in ein Daten-verarbeitungs-system

1 Wer 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.

2 Wer Passworter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

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

vom 21. Dezember 1937 (Stand am 1. Juli 2013)

Art. 144bis

Datenbeschädigung

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 311

Art. 179decies 242 Seit 1.9.2023 in Kraft

Identitätsmiss-brauch

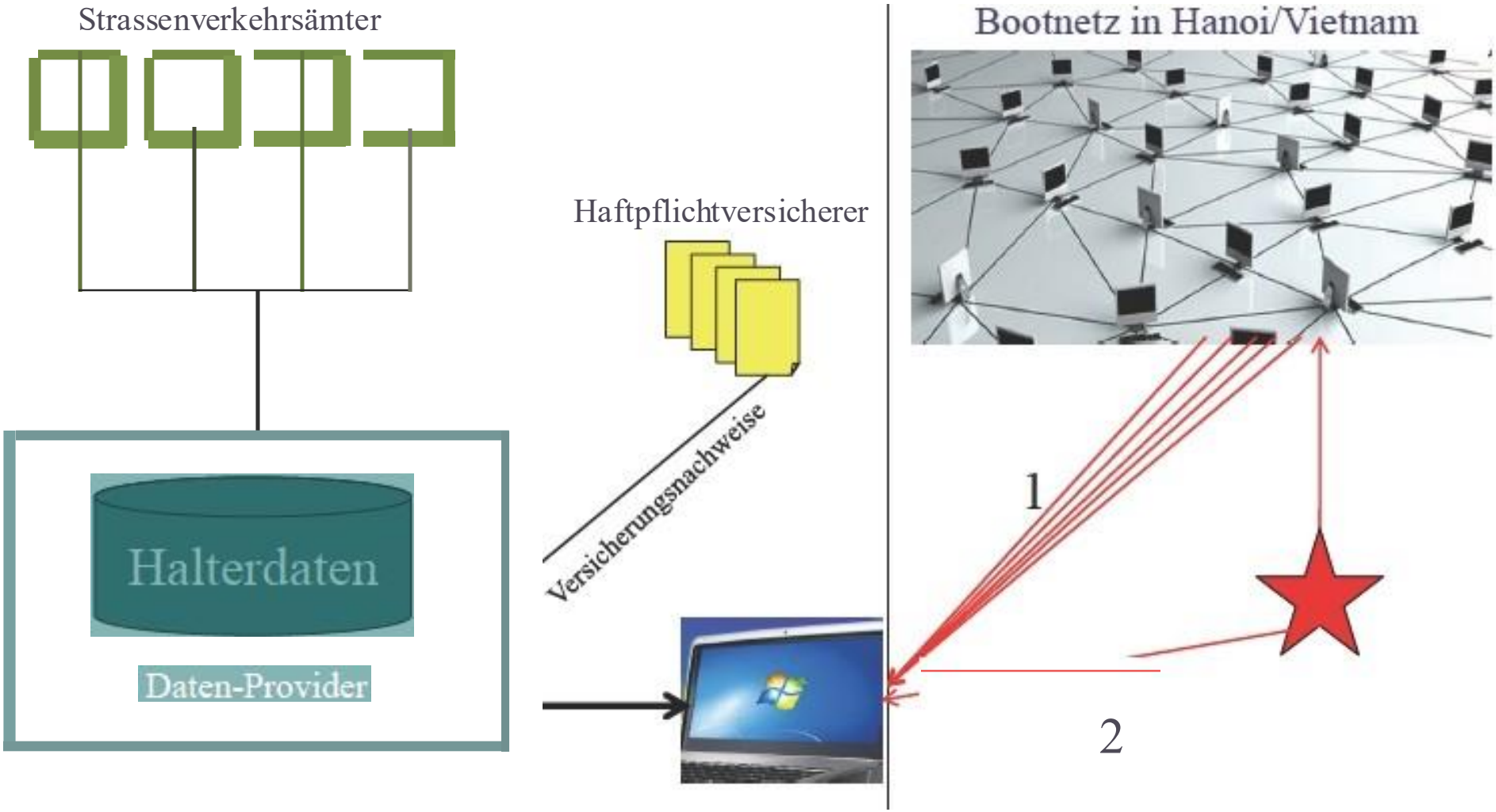
Wer die Identität einer anderen Person ohne deren Einwilligung verwendet, um dieser zu schaden oder um sich oder einem Dritten einen unrechtmässigen Vorteil zu verschaffen, wird auf Antrag mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe bestraft.

- 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

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


Strassenverkehrsämter
Halterdaten
Daten-Provider
Haftpflichtversicherer
Versicherungsnachweise
Bootnetz in Hanoi/Vietnam
1
2

InfoGuard
SWISS CYBER SECURITY

InfoGuard
SWISS CYBER SECURITY

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

KANTON LUZERN
Amtsgericht Luzern-Lond

106 EST 01

Abteilung I
Präsident Trüeb, Amtsrichterin 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 mlt 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.

Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

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 Kryptobestände. 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. Marz 2013)

Art. 13 Schutz der Privatsphäre

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

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

Schweizerisches Zivilgesetzbuch

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

II. Gegen Verletzungen
1. Grundsatz

Art. 28[30]

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

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

Schweizerisches Zivilgesetzbuch

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

Art. 28*a*[31]

2. Klage
a. Im Allgemeinen[32]

1 Der Kläger kann dem Gericht beantragen:

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

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

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz

(Datenschutzgesetz, DSG)

vom 25. September 2020

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

1. Kapitel: Zweck und Geltungsbereich sowie Aufsichtsbehörde des Bundes

Art. 1 Zweck

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

Streichung: Schutz der Daten juristischer Personen

Art. 2 Persönlicher und sachlicher Geltungsbereich

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

a. private Personen;

b. Bundesorgane.

Unternehmen sind auch private Personen

Kantone erlassen 26 Kantons-DSG

2 Es ist nicht anwendbar auf:

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

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

«$$e-seal»

«$$QrCode»

Verordnung über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

Der Schweizerische Bundesrat,

gestützt auf die Artikel 8 Absatz 3, 10 Absatz 4, 12 Absatz 5, 16 Absatz 3, 25 Absatz 6, 28 Absatz 3, 33, 59 Absätze 2 und 3 des Datenschutzgesetzes vom 25. September 2020[1] (DSG),

verordnet:

1. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Datensicherheit

Art. 1 Grundsätze

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

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

«$$e-seal»

«$$QrCode»

Verordnung über Datenschutzzertifizierungen
(VDSZ)

vom 31. August 2022

Der Schweizerische Bundesrat,

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

verordnet:

1. Abschnitt: Zertifizierungsstellen

Art. 1 Anforderungen

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

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.

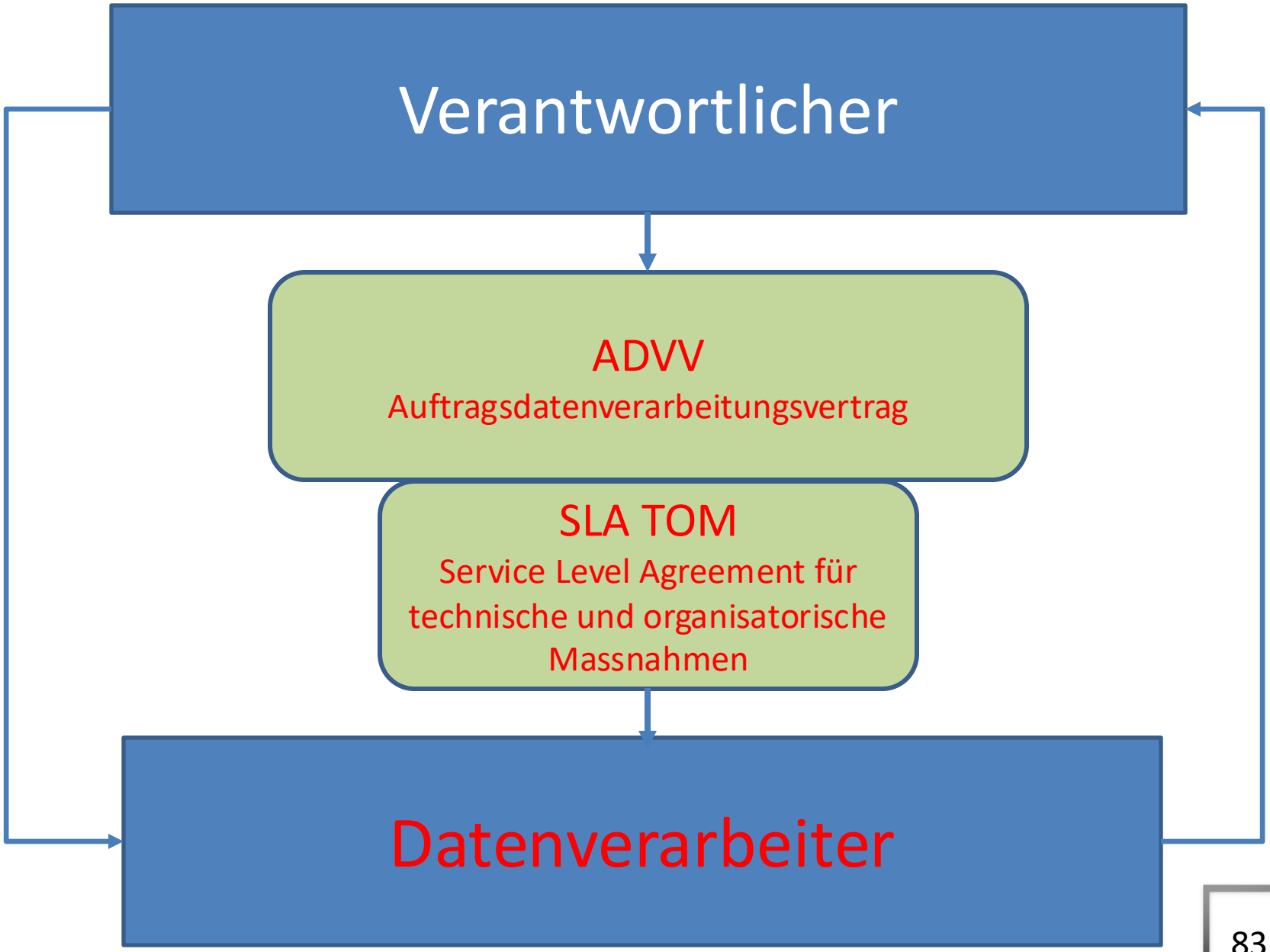
Alle Verträge mit Auftragsverarbeitern müssen überprüft und allenfalls angepasst werden.

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

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

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

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


Verantwortlicher
ADVV
Auftragsdatenverarbeitungsvertrag
SLA TOM
Service Level Agreement für technische und organisatorische Massnahmen
Datenverarbeiter

Art. 28 (4) DSGVO / 9 nDSG
Zusammenarbeit mit Auftragsverarbeiter - Drittbeizug

Zieht der Auftragsverarbeiter seinerseits

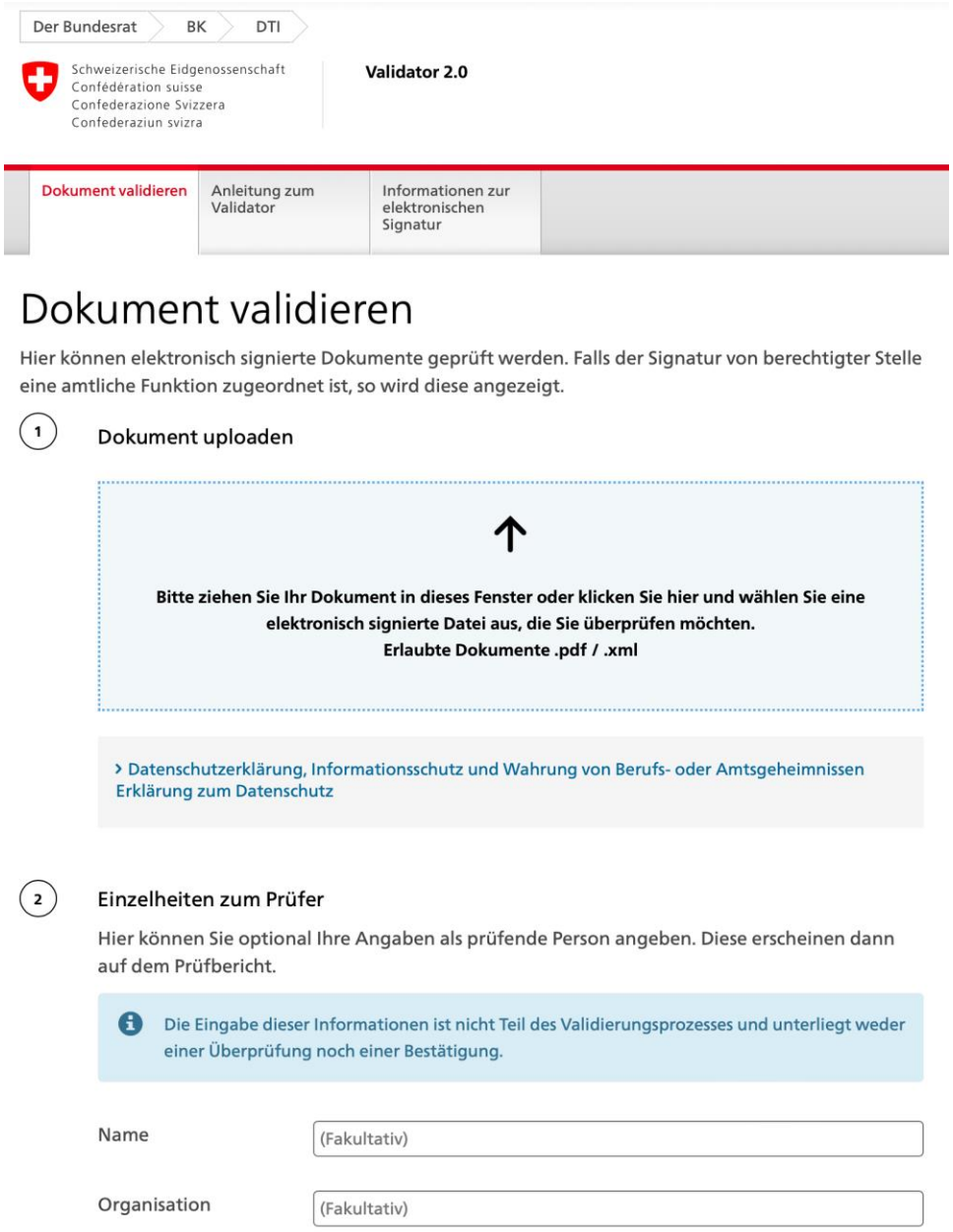
Dritte für die Verarbeitung

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)



https://www.validator.admin.ch

Meldepflichten

Data Breach Notifications (DSGVO)

§ 33 DSGVO und Art. 24 nDSG

Meldung an Datenschutzbehörde

Art. 33 DSGVO

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

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

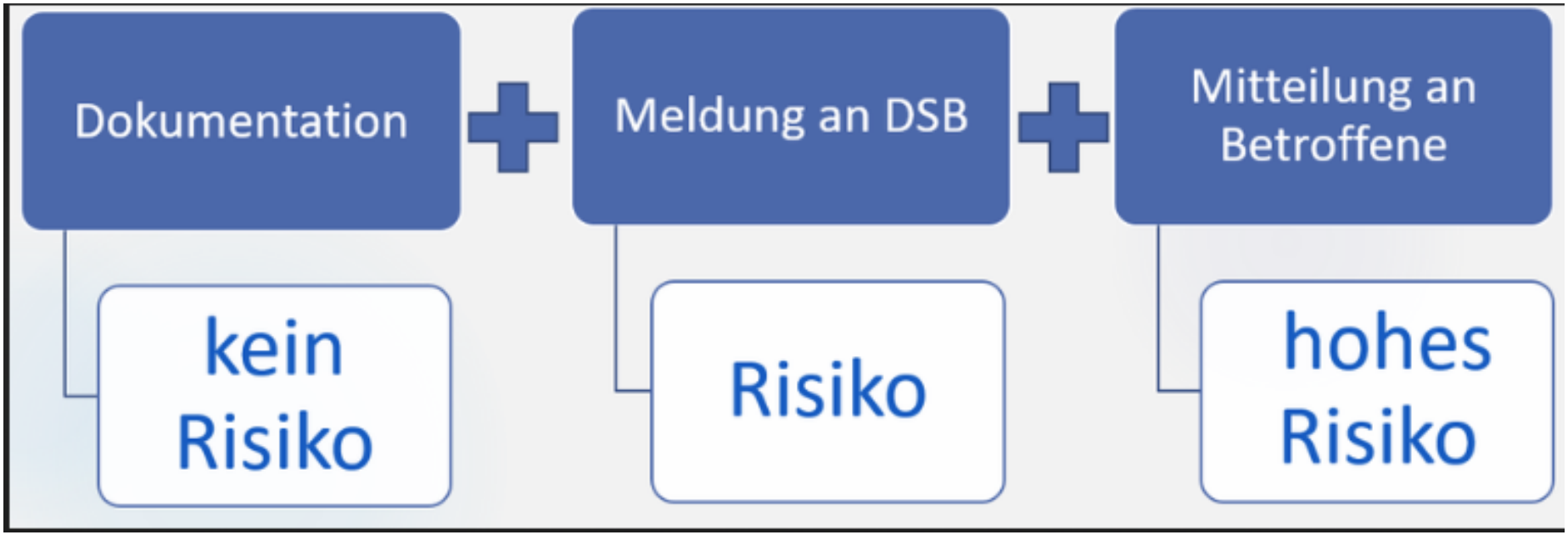
Benachrichtigung an Betroffene

Art. 34 DSGVO

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

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

Meldung und Benachrichtigung nach DSGVO



Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

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.

Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)

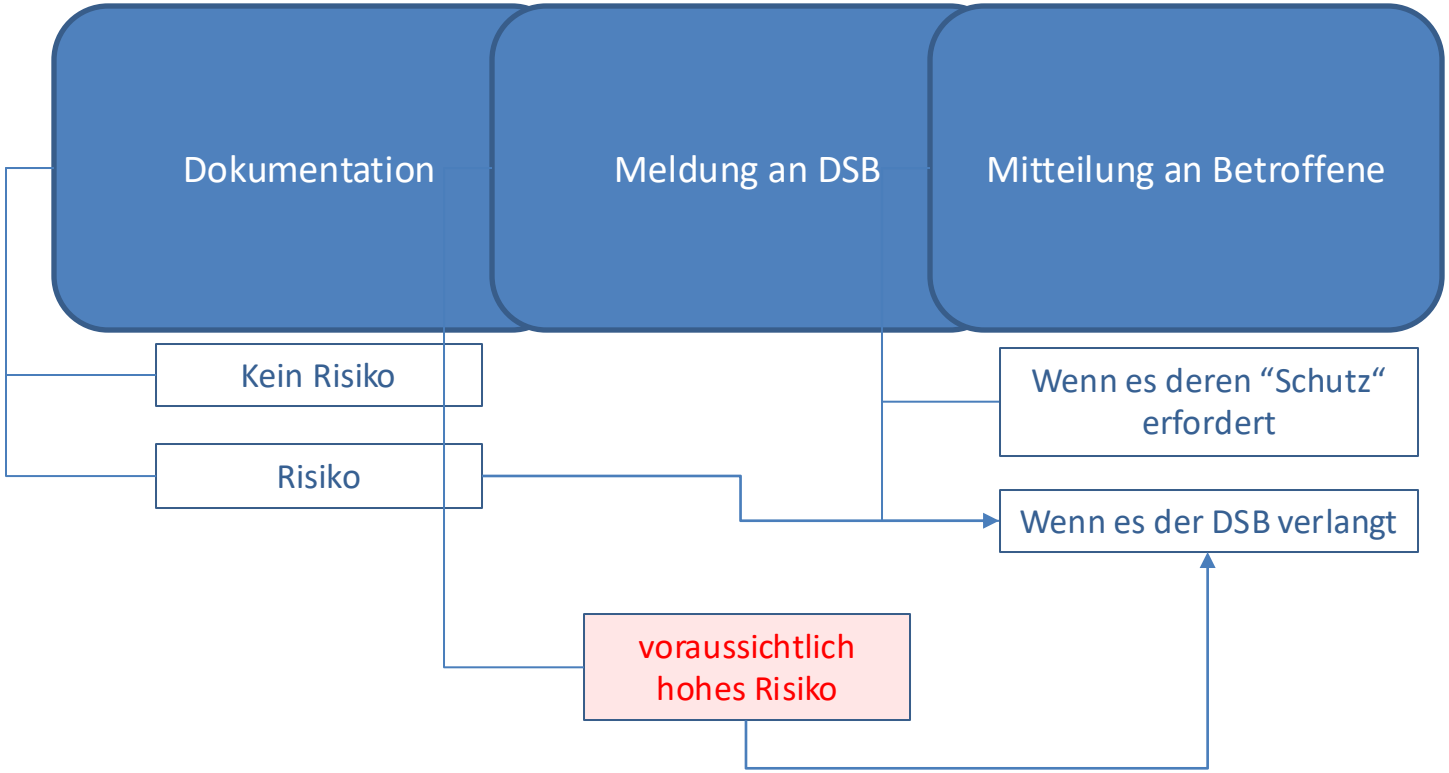
vom 31. August 2022

– Art. 15 Meldung von Verletzungen der Datensicherheit

[1] Die Meldung einer Verletzung der Datensicherheit an den EDÖB muss folgende Angaben enthalten:

a. die Art der Verletzung;
b. soweit möglich den Zeitpunkt und die Dauer;
c. soweit möglich die Kategorien und die ungefähre Anzahl der betroffenen Personendaten;
d. soweit möglich die Kategorien und die ungefähre Anzahl der betroffenen Personen;
e. die Folgen, einschliesslich der allfälligen Risiken, für die betroffenen Personen;
f. welche Massnahmen getroffen wurden oder vorgesehen sind, um den Mangel zu beheben und die Folgen, einschliesslich der allfälligen Risiken, zu mindern;
g. den Namen und die Kontaktdaten einer Ansprechperson.

Meldung und Benachrichtigung nach nDSG



Grundsätze der IT-Sicherheit im neuen Datenschutzrecht

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

---

2. Kapitel: Allgemeine Bestimmungen

1. Abschnitt: Begriffe und Grundsätze

Art. 5 Begriffe

In diesem Gesetz bedeuten:

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

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 7 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

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

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 8 Datensicherheit

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

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

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

Datenbearbeitungsvertrag mit Auftragsbearbeiter (ADVV)

Datenschutzfolgeabschätzung zwingend
TOMs ausformulieren
ADV-Übertragung der TOM auf Auftragsverarbeiter

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

Vertrags- und Auditpflichten für Verantwortlichen

Art. 9 Bearbeitung durch Auftragsbearbeiter

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

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

b. keine gesetzliche oder vertragliche Geheimhaltungspflicht die Übertragung verbietet.

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

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

Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

Art. 2 Ziele

Der Verantwortliche und der Auftragsbearbeiter müssen technische und organisatorische Massnahmen treffen, damit die bearbeiteten Daten ihrem Schutzbedarf entsprechend:

a. nur Berechtigten zugänglich sind (Vertraulichkeit);

b. verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);

c. nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);

d. nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

Art. 3 Technische und organisatorische Massnahmen

[1] Um die Vertraulichkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

a. berechtigte Personen nur auf diejenigen Personendaten Zugriff haben, die sie zur Erfüllung ihrer Aufgaben benötigen (Zugriffskontrolle);

b. nur berechtigte Personen Zugang zu den Räumlichkeiten und Anlagen haben, in denen Personendaten bearbeitet werden (Zugangskontrolle);

c. unbefugte Personen automatisierte Datenbearbeitungssysteme nicht mittels Einrichtungen zur Datenübertragung benutzen können (Benutzerkontrolle).

Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

---

[2] Um die Verfügbarkeit und Integrität zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

a. unbefugte Personen Datenträger nicht lesen, kopieren, verändern, verschieben, löschen oder vernichten können (Datenträgerkontrolle);

b. unbefugte Personen Personendaten im Speicher nicht speichern, lesen, ändern, löschen oder vernichten können (Speicherkontrolle);

c. unbefugte Personen bei der Bekanntgabe von Personendaten oder beim Transport von Datenträgern Personendaten nicht lesen, kopieren, verändern, löschen oder vernichten können (Transportkontrolle);

d. die Verfügbarkeit der Personendaten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (Wiederherstellung);

e. alle Funktionen des automatisierten Datenbearbeitungssystems zur Verfügung stehen (Verfügbarkeit), Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität);

f. Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit).

Verordnung
über den Datenschutz
(Datenschutzverordnung, DSV)

vom 31. August 2022

---

[3] Um die Nachvollziehbarkeit zu gewährleisten, müssen der Verantwortliche und der Auftragsbearbeiter geeignete Massnahmen treffen, damit:

a. überprüft werden kann, welche Personendaten zu welcher Zeit und von welcher Person im automatisierten Datenbearbeitungssystem eingegeben oder verändert werden (Eingabekontrolle);

b. überprüft werden kann, wem Personendaten mit Hilfe von Einrichtungen zur Datenübertragung bekanntgegeben werden (Bekanntgabekontrolle);

c. Verletzungen der Datensicherheit rasch erkannt (Erkennung) und Massnahmen zur Minderung oder Beseitigung der Folgen ergriffen werden können (Beseitigung).

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

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

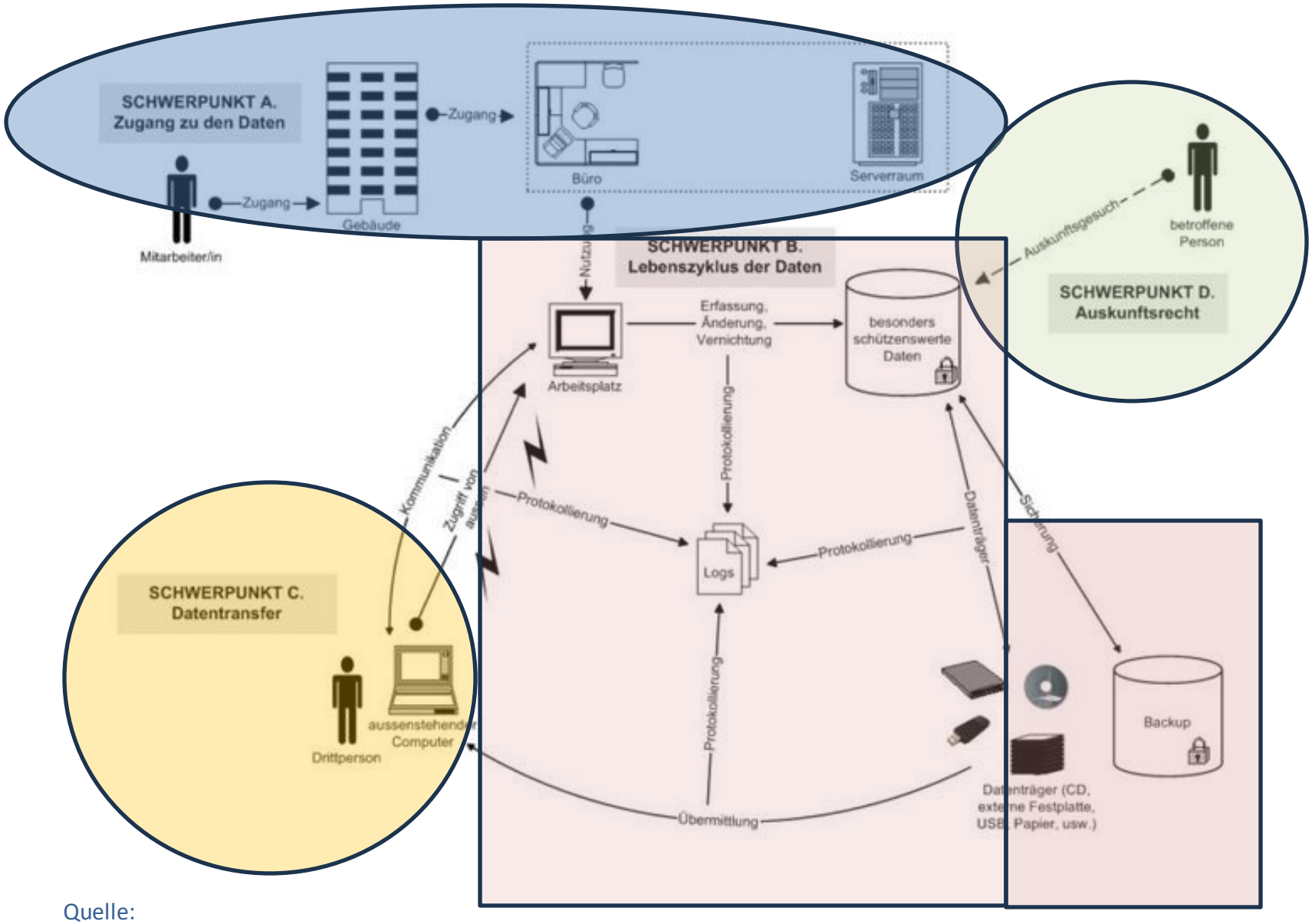
15. Januar 2024

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

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

15. Januar 2024

INHALTSVERZEICHNIS



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

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

22. Januar 2025

mit Ergänzung vom 6. Oktober 2025

Version	Datum	Beschreibung
1.0	22.01.2025	Erste finalisierte Version
1.1	06.10.2025	Ergänzung Fussnote 5, Ergänzung eines Satzes im Absatz 3 in Ziff. 3.1.2, Ergänzung im letzten Satz von Ziff. 3.2.2, Präzisierende Ergänzungen und Anpassungen in Ziff. 3.5.2, Präzisierende Ergänzungen in Ziff. 3.6, Ergänzung in Ziffer 3.8.1, Ergänzung eines Verweises im letztem Satz des ersten Absatzes in Ziff. 3.9, Präzisierende Ergänzungen in Ziff. 3.10.1, Ergänzungen und Präzisierung in Ziff. 3.11.1, Präzisierung erster Satz in Ziff. 3.11.3 betr. eingebettete Dritte, Ergänzung eines zweiten Absatzes in Ziff. 3.12.3, Präzisierung in Ziff. 3.12.4. betreffend Gratisdienstleistungen und Cookie Paywalls.

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

Insbesondere fand es der EDÖB nützlich zu verdeutlichen, warum der Einsatz von Cookies zum Zwecke der Zustellung von personalisierter Werbung unter Umständen die Einwilligung der betroffenen Personen erfordert. So, wenn der Webseitenbetreiber mittels Einbindung von Third-Party-Cookies oder ähnlicher Technologien Dritten Zugang zu personenbezogenen Informationen der Besuchenden gegen Entgelt verschafft und diese Dritten in mehrere Webseiten eingebettet sind. Da Letztere somit in die Lage versetzt werden, ein Profiling mit hohem Risiko durchzuführen, stellt dies einen besonders intensiven Eingriff in die Persönlichkeit der betroffenen Personen dar.

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

Auch brachte der EDÖB Ergänzungen zum Thema der Erhebung von Standortdaten vor – einer Datenbearbeitung, die sehr verbreitet ist und besondere Risiken mit sich bringt: Sie begünstigt einerseits die Bestimmbarkeit der realen Identität eines Onlinenutzers (zum Beispiel indem rekonstruiert werden kann, wo sich ein Gerät während der Nacht bzw. Schlafenszeit befindet, oder an welchen Adressen es sich an Werktagen regelmässig befindet). Andererseits eröffnen Standortdaten die Möglichkeit, Rückschlüsse über wesentliche Aspekte der Persönlichkeit der Nutzer zu ziehen. Ein Profiling, das sich auf Standortdaten stützt, stellt somit oft ein Profiling mit hohem Risiko dar.

Leitfaden des EDÖB betreffend Datenbearbeitungen mittels Cookies und ähnlichen Technologien

Weiter thematisiert die aktualisierte Fassung des Leitfadens den Einsatz von sog. Cookie-Paywalls. Sie legt dar, ob und unter welchen Umständen eine Einwilligung rechtsgültig erteilt werden kann, wenn die betroffene Person vor die Wahl gestellt wird, ihre Einwilligung zu erteilen oder ein bezahltes Abonnement abzuschliessen.

Neue Standard-Bestimmungen zur Informationssicherheit

SEPOS: Standardbestimmungen Informationssicherheit in Beschaffungsverträgen

Die Fachstelle des Bundes für Informationssicherheit im Staatssekretariat für Sicherheitspolitik SEPOS hat im Auftrag des Bundesrats **Standardbestimmungen für die Informationssicherheit für Beschaffungsverträge** veröffentlicht, um die Informationssicherheit des Bundes zu erhöhen und Datenabflüsse bei Lieferanten zu verhindern (die Lehren aus Xplain waren leitend).

Die Standardbestimmungen verstehen sich als **Empfehlung** an die Bedarfs- und Beschaffungsstellen des Bundes und sind per **1. Januar 2026** wirksam.

Zur konkreten Anwendung enthält das Dokument mit Leitfaden und Kommentare Standardbestimmungen eine verschachtelte Prüfreihenfolge, die eine Kombination aus AGB und Standardbestimmungen empfiehlt, je nach Sensitivität der vom Dienstleister bearbeiteten Informationen, nach Art und Delivery der Dienstleistung und nach dem Personenbezug bearbeiteter Daten.

https://datenrecht.ch/sepos-standardbestimmungen-informationssicherheit-in-beschaffungsvertraegen/?utm_source=datenrecht&utm_campaign=13296bf40b-datenrecht-Mailchimp&utm_medium=email&utm_term=0_15155ce73b-13296bf40b-90792857

Standardbestimmungen Informationssicherheit in Beschaffungsverträgen (2)

Sie **ergänzen die AGB des Bundes** (siehe hier) und umfassen die folgenden Bestimmungen:

- H1 Standardbestimmung ohne Bezug zu Informatikmitteln des Bundes mit Abgabe von Bundesgeräten
- H2 Standardbestimmung ohne Bezug zu Informatikmitteln des Bundes ohne Abgabe von Bundesgeräten
- I1 Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Verwaltung, Wartung, Überprüfung) mit Abgabe von Bundesgeräten
- I2 Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Verwaltung, Wartung, Überprüfung) ohne Abgabe von Bundesgeräten
- J Standardbestimmung mit Bezug zu Informatikmitteln des Bundes (Betrieb)

Standardbestimmungen Informationssicherheit in Beschaffungsverträgen (3)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Staatssekretariat für Sicherheitspolitik SEPOS

Leitfaden
für die Verwendung der Standardbestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1])

I. Einführung

Der vorliegende Leitfaden soll es den Bedarfsstellen nach Artikel 2 Buchstabe c Org-VöB[2] erlauben, im Bereich der Informationssicherheit bei allen Beschaffungs- und Dienstleistungsverträgen die Anbieterinnen zielgerichtet mittels standardisierter, vorformulierter Bestimmungen (in der Folge «Standardbestimmung(en)» genannt) zu instruieren, wie mit Informationen oder Informatikmitteln des Bundes bei der Erbringung ihrer vertraglichen Leistung umzugehen ist.

II. Kategorisierung der Beschaffungs- und Dienstleistungsverträge

Beschaffungs- und Dienstleistungsverträge können inhaltlich vielerlei Gestalt haben, weshalb es unmöglich ist – nach dem Motto «One for all» – eine einzige, allgemeingültige Standardbestimmung zu verwenden. Selbst eine schematische Anwendung einer kleinen, geschlossenen Anzahl standardisierter Inhalte erfordert eine vorgängige Kategorisierung der Verträge (nachfolgend Kategorien 1–4).

Innerhalb der Kategorien muss wiederum zwischen verschiedenen **Anwendungsfällen** (a–d) unterschieden werden:

Buchstabe a: Der Beschaffungsvertrag beinhaltet die Bearbeitung von Informationen des Bundes, wobei keine Verwaltung, kein Betrieb, keine Wartung, keine Entwicklung und keine Überprüfung von Informatikmitteln des Bundes im Sinn der nachfolgenden Buchstaben b und c erfolgt.

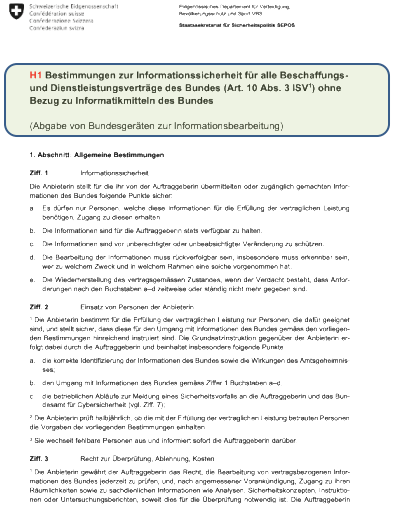
Buchstabe b: Der Beschaffungsvertrag beinhaltet die Verwaltung, die Wartung, die Entwicklung oder die Überprüfung von Informatikmitteln des Bundes (nicht den Betrieb). Inhaber (Besitzer/Eigentümer) dieser Informatikmittel ist der Bund. Diese Arbeiten werden mit betrieblichen Informatikmitteln (Eigentum/Besitz bei der Anbieterin) oder Bundesgeräten vorgenommen und es können davon auch Informationen des Bundes oder Personendaten betroffen sein. Die unter den genannten Begriffen zu verstehenden Tätigkeiten müssen geeignet sein, so auf eine Hard- oder Software einzuwirken, dass dadurch die Vertraulichkeit, die Verfügbarkeit, die Integrität oder die Nachvollziehbarkeit der Informationen des Bundes beeinträchtigt werden können (z. B. Administratoren). Die einfache Bearbeitung der Informationen mit dem Informatikmittel fällt unter den Buchstaben a.

Buchstabe c: Der Beschaffungsvertrag beinhaltet eine eigentliche Informatik-Leistungserbringung (Betrieb) durch die Anbieterin mit deren betrieblichen Informatikmitteln und es können davon auch Informationen des Bundes oder Personendaten betroffen sein. Das heisst, die Informationen des Bundes werden auf Servern oder in Rechenzentren (Informatikmitteln) gehalten, deren Inhaberin (Besitzerin/Eigentümerin) im Gegensatz zu Buchstabe b die Anbieterin ist und auf die die Auftraggeberin keinen eigenen Zugriff hat (z. B. Cloud-Services).

Buchstabe d: Zur Erfüllung der vertraglichen Leistung werden betriebliche Informatikmittel der Anbieterin oder vom Bund zur Verfügung gestellte Geräte verwendet.

[1] Informationssicherheitsverordnung (SR 128.1)

[2] Verordnung über die Organisation des öffentlichen Beschaffungswesens der Bundesverwaltung (SR 172.056.15)



H1 Bestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1]) ohne Bezug zu Informatikmitteln des Bundes

(Abgabe von Bundesgeräten zur Informationsbearbeitung)

1. Abschnitt Allgemeine Bestimmungen

Ziff. 1 Informationssicherheit

Die Anbieterin stellt für die ihr von der Auftraggeberin übermittelten oder zugänglich gemachten Informationen des Bundes folgende Punkte sicher:

a. Es dürfen nur Personen, welche diese Informationen für die Erfüllung der vertraglichen Leistung benötigen, Zugang zu diesen erhalten.
b. Die Informationen sind für die Auftraggeberin stets verfügbar zu halten.
c. Die Informationen sind vor unberechtigter oder unbeabsichtigter Veränderung zu schützen.
d. Die Bearbeitung der Informationen muss rückverfolgbar sein, insbesondere muss erkennbar sein, wer zu welchem Zweck und in welchem Rahmen eine solche vorgenommen hat.
e. Die Wiederherstellung des vertragsgemässen Zustandes, wenn der Verdacht besteht, dass Anforderungen nach den Buchstaben a–d zeitweise oder ständig nicht mehr gegeben sind.

Ziff. 2 Einsatz von Personen der Anbieterin

[1] Die Anbieterin bestimmt für die Erfüllung der vertraglichen Leistung nur Personen, die dafür geeignet sind, und stellt sicher, dass diese für den Umgang mit Informationen des Bundes gemäss den vorliegenden Bestimmungen hinreichend instruiert sind. Die Grundsatzinstruktion gegenüber der Anbieterin erfolgt dabei durch die Auftraggeberin und beinhaltet insbesondere folgende Punkte:

a. die korrekte Identifizierung der Informationen des Bundes sowie die Wirkungen des Amtsgeheimnisses;
b. den Umgang mit Informationen des Bundes gemäss Ziffer 1 Buchstaben a–d;
c. die betrieblichen Abläufe zur Meldung eines Sicherheitsvorfalls an die Auftraggeberin und das Bundesamt für Cybersicherheit (vgl. Ziff. 7).

[2] Die Anbieterin prüft halbjährlich, ob die mit der Erfüllung der vertraglichen Leistung betrauten Personen die Vorgaben der vorliegenden Bestimmungen einhalten.

[3] Sie wechselt fehlbare Personen aus und informiert sofort die Auftraggeberin darüber.

Ziff. 3 Recht zur Überprüfung, Ablehnung, Kosten

[1] Die Anbieterin gewährt der Auftraggeberin das Recht, die Bearbeitung von vertragsbezogenen Informationen des Bundes jederzeit zu prüfen, und, nach angemessener Vorankündigung, Zugang zu ihren Räumlichkeiten sowie zu sachdienlichen Informationen wie Analysen, Sicherheitskonzepten, Instruktionen oder Untersuchungsberichten, soweit dies für die Überprüfung notwendig ist. Die Auftraggeberin verzichtet in dem Umfang auf das Recht zur Überprüfung, in welchem die Anbieterin nachweisen kann, dass sie gegenüber Dritten gesetzlich oder vertraglich zur Geheimhaltung verpflichtet ist.

[1] Informationssicherheitsverordnung (SR 128.1)

I1 Bestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1]) mit Bezug zu Verwaltung, Wartung, Entwicklung und Überprüfung von Informatikmitteln des Bundes der Sicherheitsstufe «Grundschutz»

(Abgabe von Bundesgeräten zur Informationsbearbeitung)

1. Abschnitt Allgemeine Bestimmungen

Ziff. 1 Informationssicherheit

[1] Die Anbieterin stellt bei der Verwaltung, Wartung, Entwicklung und/oder Überprüfung des Informatikmittels des Bundes folgende Punkte sicher, wenn im Zuge der Erfüllung der vertraglichen Leistung Zugriff auf oder Einsichtnahme in Informationen des Bundes unvermeidlich sind:

a. Der Kreis der Personen, welche bei der Erfüllung der vertraglichen Leistung Informationen des Bundes einsehen können, ist auf ein Minimum zu beschränken.
b. Die Informationen sind für die Auftraggeberin stets verfügbar zu halten.
c. Die Informationen sind vor unberechtigter oder unbeabsichtigter Veränderung zu schützen.
d. Die Wiederherstellung des vertragsgemässen Zustandes, wenn der Verdacht besteht, dass Anforderungen nach den Buchstaben a–c zeitweise oder ständig nicht mehr gegeben sind.

[2] Die Bearbeitung von Informationen des Bundes ist grundsätzlich untersagt. Eine Ausnahme besteht nur dann, wenn die Bearbeitung explizit als Vertragsgegenstand definiert oder für die Erfüllung der vertraglichen Leistung unabdingbar ist. Die Bearbeitung der Informationen muss rückverfolgbar sein, insbesondere muss erkennbar sein, wer zu welchem Zweck und in welchem Rahmen eine solche vorgenommen hat.

Ziff. 2 Einsatz von Personen der Anbieterin

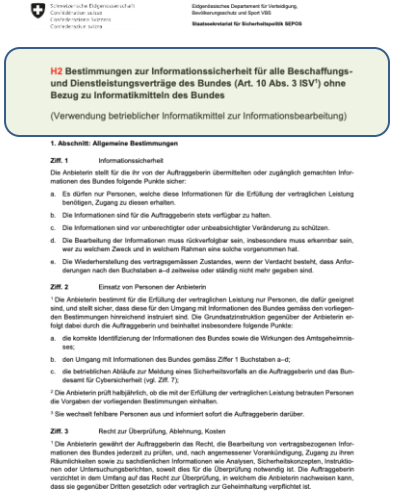
[1] Die Anbieterin bestimmt für die Erfüllung der vertraglichen Leistung nur Personen, die dafür geeignet sind, und stellt sicher, dass diese für den Umgang mit Informationen des Bundes gemäss den vorliegenden Bestimmungen hinreichend instruiert sind. Die Grundsatzinstruktion gegenüber der Anbieterin erfolgt dabei durch die Auftraggeberin und beinhaltet insbesondere folgende Punkte:

a. die korrekte Identifizierung der Informationen des Bundes sowie die Wirkungen des Amtsgeheimnisses;
b. den Umgang mit Informationen des Bundes gemäss Ziffer 1 Buchstaben a–c;
c. die betrieblichen Abläufe zur Meldung eines Sicherheitsvorfalls an die Auftraggeberin und das Bundesamt für Cybersicherheit (vgl. Ziff. 7).

[2] Die Anbieterin prüft halbjährlich, ob die mit der Erfüllung der vertraglichen Leistung betrauten Personen die Vorgaben der vorliegenden Bestimmungen einhalten.

[3] Sie wechselt fehlbare Personen aus und informiert sofort die Auftraggeberin darüber.

[1] Informationssicherheitsverordnung (SR 128.1)



H2 Bestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1]) ohne Bezug zu Informatikmitteln des Bundes

(Verwendung betrieblicher Informatikmittel zur Informationsbearbeitung)

1. Abschnitt: Allgemeine Bestimmungen

Ziff. 1 Informationssicherheit

Die Anbieterin stellt für die ihr von der Auftraggeberin übermittelten oder zugänglich gemachten Informationen des Bundes folgende Punkte sicher:

a. Es dürfen nur Personen, welche diese Informationen für die Erfüllung der vertraglichen Leistung benötigen, Zugang zu diesen erhalten.
b. Die Informationen sind für die Auftraggeberin stets verfügbar zu halten.
c. Die Informationen sind vor unberechtigter oder unbeabsichtigter Veränderung zu schützen.
d. Die Bearbeitung der Informationen muss rückverfolgbar sein, insbesondere muss erkennbar sein, wer zu welchem Zweck und in welchem Rahmen eine solche vorgenommen hat.
e. Die Wiederherstellung des vertragsgemässen Zustandes, wenn der Verdacht besteht, dass Anforderungen nach den Buchstaben a–d zeitweise oder ständig nicht mehr gegeben sind.

Ziff. 2 Einsatz von Personen der Anbieterin

[1] Die Anbieterin bestimmt für die Erfüllung der vertraglichen Leistung nur Personen, die dafür geeignet sind, und stellt sicher, dass diese für den Umgang mit Informationen des Bundes gemäss den vorliegenden Bestimmungen hinreichend instruiert sind. Die Grundsatzinstruktion gegenüber der Anbieterin erfolgt dabei durch die Auftraggeberin und beinhaltet insbesondere folgende Punkte:

a. die korrekte Identifizierung der Informationen des Bundes sowie die Wirkungen des Amtsgeheimnisses;
b. den Umgang mit Informationen des Bundes gemäss Ziffer 1 Buchstaben a–d;
c. die betrieblichen Abläufe zur Meldung eines Sicherheitsvorfalls an die Auftraggeberin und das Bundesamt für Cybersicherheit (vgl. Ziff. 7).

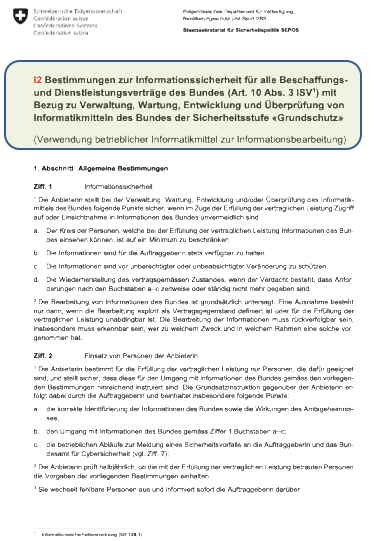
[2] Die Anbieterin prüft halbjährlich, ob die mit der Erfüllung der vertraglichen Leistung betrauten Personen die Vorgaben der vorliegenden Bestimmungen einhalten.

[3] Sie wechselt fehlbare Personen aus und informiert sofort die Auftraggeberin darüber.

Ziff. 3 Recht zur Überprüfung, Ablehnung, Kosten

[1] Die Anbieterin gewährt der Auftraggeberin das Recht, die Bearbeitung von vertragsbezogenen Informationen des Bundes jederzeit zu prüfen, und, nach angemessener Vorankündigung, Zugang zu ihren Räumlichkeiten sowie zu sachdienlichen Informationen wie Analysen, Sicherheitskonzepten, Instruktionen oder Untersuchungsberichten, soweit dies für die Überprüfung notwendig ist. Die Auftraggeberin verzichtet in dem Umfang auf das Recht zur Überprüfung, in welchem die Anbieterin nachweisen kann, dass sie gegenüber Dritten gesetzlich oder vertraglich zur Geheimhaltung verpflichtet ist.

[1] Informationssicherheitsverordnung (SR 128.1)



I2 Bestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1]) mit Bezug zu Verwaltung, Wartung, Entwicklung und Überprüfung von Informatikmitteln des Bundes der Sicherheitsstufe «Grundschutz»

(Verwendung betrieblicher Informatikmittel zur Informationsbearbeitung)

1. Abschnitt Allgemeine Bestimmungen

Ziff. 1 Informationssicherheit

[1] Die Anbieterin stellt bei der Verwaltung, Wartung, Entwicklung und/oder Überprüfung des Informatikmittels des Bundes folgende Punkte sicher, wenn im Zuge der Erfüllung der vertraglichen Leistung Zugriff auf oder Einsichtnahme in Informationen des Bundes unvermeidlich sind:

a. Der Kreis der Personen, welche bei der Erfüllung der vertraglichen Leistung Informationen des Bundes einsehen können, ist auf ein Minimum zu beschränken.
b. Die Informationen sind für die Auftraggeberin stets verfügbar zu halten.
c. Die Informationen sind vor unberechtigter oder unbeabsichtigter Veränderung zu schützen.
d. Die Wiederherstellung des vertragsgemässen Zustandes, wenn der Verdacht besteht, dass Anforderungen nach den Buchstaben a–c zeitweise oder ständig nicht mehr gegeben sind.

[2] Die Bearbeitung von Informationen des Bundes ist grundsätzlich untersagt. Eine Ausnahme besteht nur dann, wenn die Bearbeitung explizit als Vertragsgegenstand definiert ist oder für die Erfüllung der vertraglichen Leistung unabdingbar ist. Die Bearbeitung der Informationen muss rückverfolgbar sein, insbesondere muss erkennbar sein, wer zu welchem Zweck und in welchem Rahmen eine solche vorgenommen hat.

Ziff. 2 Einsatz von Personen der Anbieterin

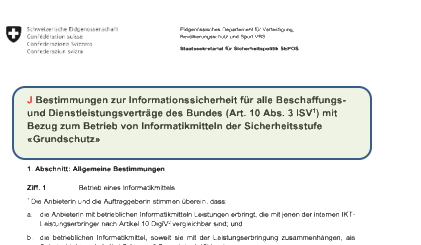
[1] Die Anbieterin bestimmt für die Erfüllung der vertraglichen Leistung nur Personen, die dafür geeignet sind, und stellt sicher, dass diese für den Umgang mit Informationen des Bundes gemäss den vorliegenden Bestimmungen hinreichend instruiert sind. Die Grundsatzinstruktion gegenüber der Anbieterin erfolgt dabei durch die Auftraggeberin und beinhaltet insbesondere folgende Punkte:

a. die korrekte Identifizierung der Informationen des Bundes sowie die Wirkungen des Amtsgeheimnisses;
b. den Umgang mit Informationen des Bundes gemäss Ziffer 1 Buchstaben a–c;
c. die betrieblichen Abläufe zur Meldung eines Sicherheitsvorfalls an die Auftraggeberin und das Bundesamt für Cybersicherheit (vgl. Ziff. 7).

[2] Die Anbieterin prüft halbjährlich, ob die mit der Erfüllung der vertraglichen Leistung betrauten Personen die Vorgaben der vorliegenden Bestimmungen einhalten.

[3] Sie wechselt fehlbare Personen aus und informiert sofort die Auftraggeberin darüber.

[1] Informationssicherheitsverordnung (SR 128.1)



J Bestimmungen zur Informationssicherheit für alle Beschaffungs- und Dienstleistungsverträge des Bundes (Art. 10 Abs. 3 ISV[1]) mit Bezug zum Betrieb von Informatikmitteln der Sicherheitsstufe «Grundschutz»

1. Abschnitt: Allgemeine Bestimmungen

Ziff. 1 Betrieb eines Informatikmittels

[1] Die Anbieterin und die Auftraggeberin stimmen überein, dass:

a. die Anbieterin mit betrieblicher Informatikmittel Leistungen erbringt, die mit jenen der internen IKT-Leistungserbringer nach Artikel 10 OgIV vergleichbar sind; und
b. die betriebliche Informatikmittel, soweit sie mit der Leistungserbringung zusammenhängen, als Schutzobjekt nach Artikel 7 Absatz 2 Buchstabe b ISV gelten.

[2] Als betriebliche Informatikmittel gelten Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme sowie Einrichtungen, Produkte und Dienste, die der elektronischen Verarbeitung von Informationen zum Zweck der Erfüllung der vertraglichen Leistung dienen und deren Verwaltung, Betrieb, Wartung und Überprüfung in der Verantwortung der Anbieterin liegt oder deren Eigentümerin sie ist.

[3] Die Kosten für Verwaltung, Betrieb, Wartung und Überprüfung betrieblicher Informatikmittel gehen zu Lasten der Anbieterin.

Ziff. 2 Informationssicherheit

[1] Die Anbieterin stellt beim Betrieb des betrieblichen Informatikmittels folgende Punkte sicher, wenn im Zuge der Erfüllung der vertraglichen Leistung Zugriff auf oder Einsichtnahme in Informationen des Bundes unvermeidlich sind:

a. Der Kreis der Personen, welche bei der Erfüllung der vertraglichen Leistung Informationen des Bundes einsehen können, ist auf ein Minimum zu beschränken.
b. Die Informationen sind für die Auftraggeberin stets verfügbar zu halten.
c. Die Informationen sind vor unberechtigter oder unbeabsichtigter Veränderung zu schützen.
d. Die Wiederherstellung des vertragsgemässen Zustandes, wenn der Verdacht besteht, dass Anforderungen nach den Buchstaben a–c zeitweise oder ständig nicht mehr gegeben sind.

[1] Die Bearbeitung von Informationen des Bundes ist grundsätzlich untersagt. Eine Ausnahme besteht nur dann, wenn die Bearbeitung explizit als Vertragsgegenstand definiert ist oder für die Erfüllung der vertraglichen Leistung unabdingbar ist. Die Bearbeitung der Informationen muss rückverfolgbar sein, insbesondere muss erkennbar sein, wer zu welchem Zweck und in welchem Rahmen eine solche vorgenommen hat.

[1] Informationssicherheitsverordnung (SR 128.1)

[2] Digitalisierungsverordnung (SR 172.010.1)

Cloud-Computing und Auslandspeicherung

Bekanntgabe Personendaten ins Ausland

3. Abschnitt: Bekanntgabe von Personendaten ins Ausland

Art. 16 Grundsätze

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

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

a. einen völkerrechtlichen Vertrag;

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

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

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

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

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

Bekanntgabe Personendaten ins Ausland

Art. 17 Ausnahmen

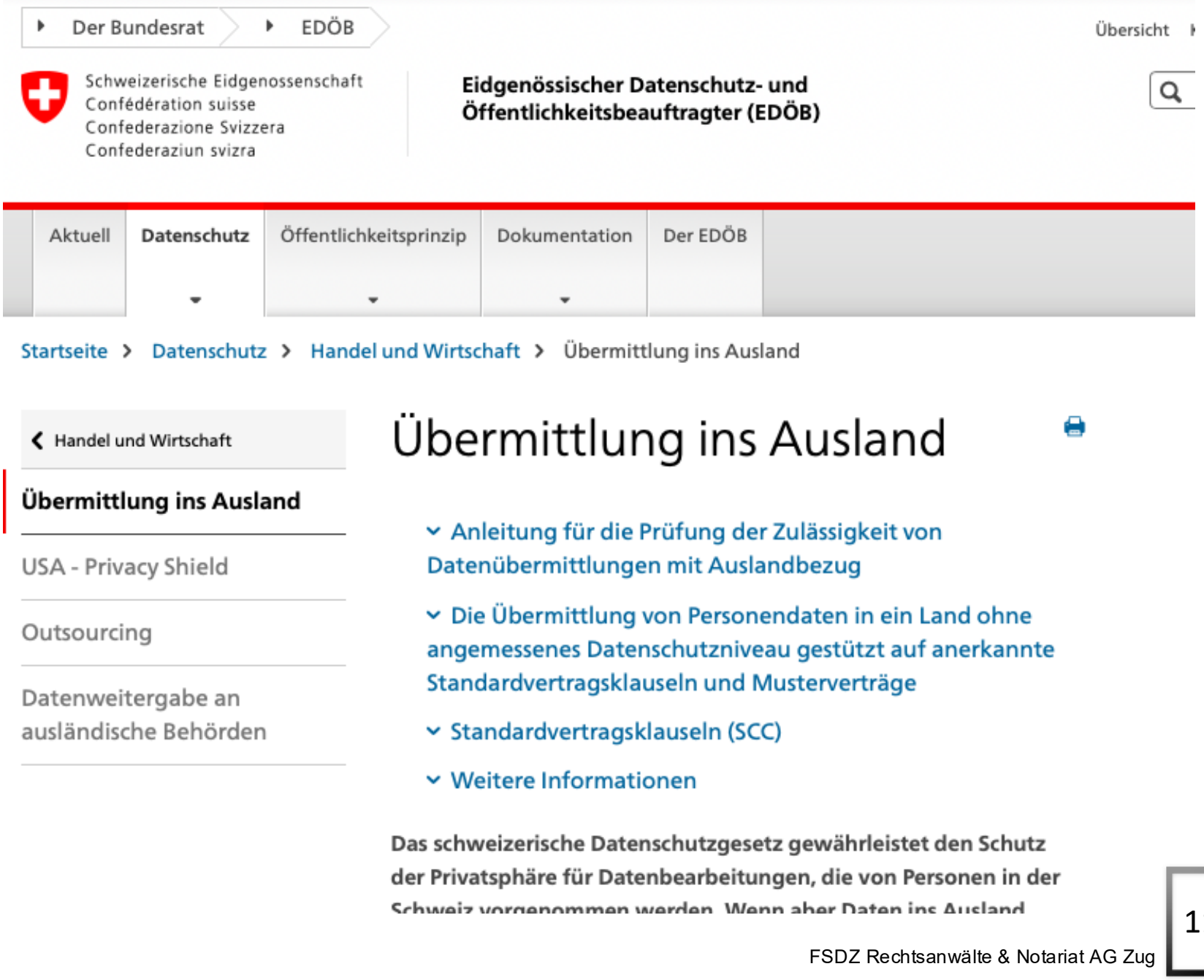
[1] Abweichend von Artikel 16 Absätze 1 und 2 dürfen in den folgenden Fällen Personendaten ins Ausland bekanntgegeben werden:

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

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

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

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


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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

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

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

1. Zweck der Anleitung

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

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

Beilage:
„Die Übermittlung von Personendaten in ein Land ohne angemessenes Datenschutzniveau gestützt auf Standarddatenschutzklauseln nach Art. 16 Abs. 2 lit. d DSG» in den Unterlagen.

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

Verordnung über den Datenschutz (Datenschutzverordnung, DSV)

235.11

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

Art. 8 Beurteilung der Angemessenheit des Datenschutzes eines Staates, eines Gebiets, eines spezifischen Sektors in einem Staat oder eines internationalen Organs

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

Anhang 1
(Art. 8 Abs. 1)

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

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

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

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

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

https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anerkennung-staaten.html

SCC - Standard Contractual Clauses der EU

ANHANG I

A. **LISTE DER PARTEIEN**

MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche

MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter

MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter

MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

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

1. Name: .....

   Anschrift: .....

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

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

   Unterschrift und Datum: .....

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

2. .....

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

1. Name: .....

   Anschrift: .....

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

Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer

Page contents

- Einzelheiten
- Beschreibung
- Dateien

Einzelheiten

Datum der Veröffentlichung	4. Juni 2021
Autor	Generaldirektion Justiz und Verbraucher
Beteiligte dienststelle	Generaldirektion Justiz und Verbraucher

Beschreibung

Haftungsausschluss: Diese Texte sind endgültige Arbeitsdokumente. Der einzige offizielle Text wird in den kommenden Tagen im Amtsblatt veröffentlicht.

DURCHFÜHRUNGSBESCHLUSS DER KOMMISSION über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679

Dateien

Standard Contractual Clauses for controllers and processors in the EU/EEA

25. MAI 2022

Standard contractual clauses for controllers and processors in the EU/EEA (Word)

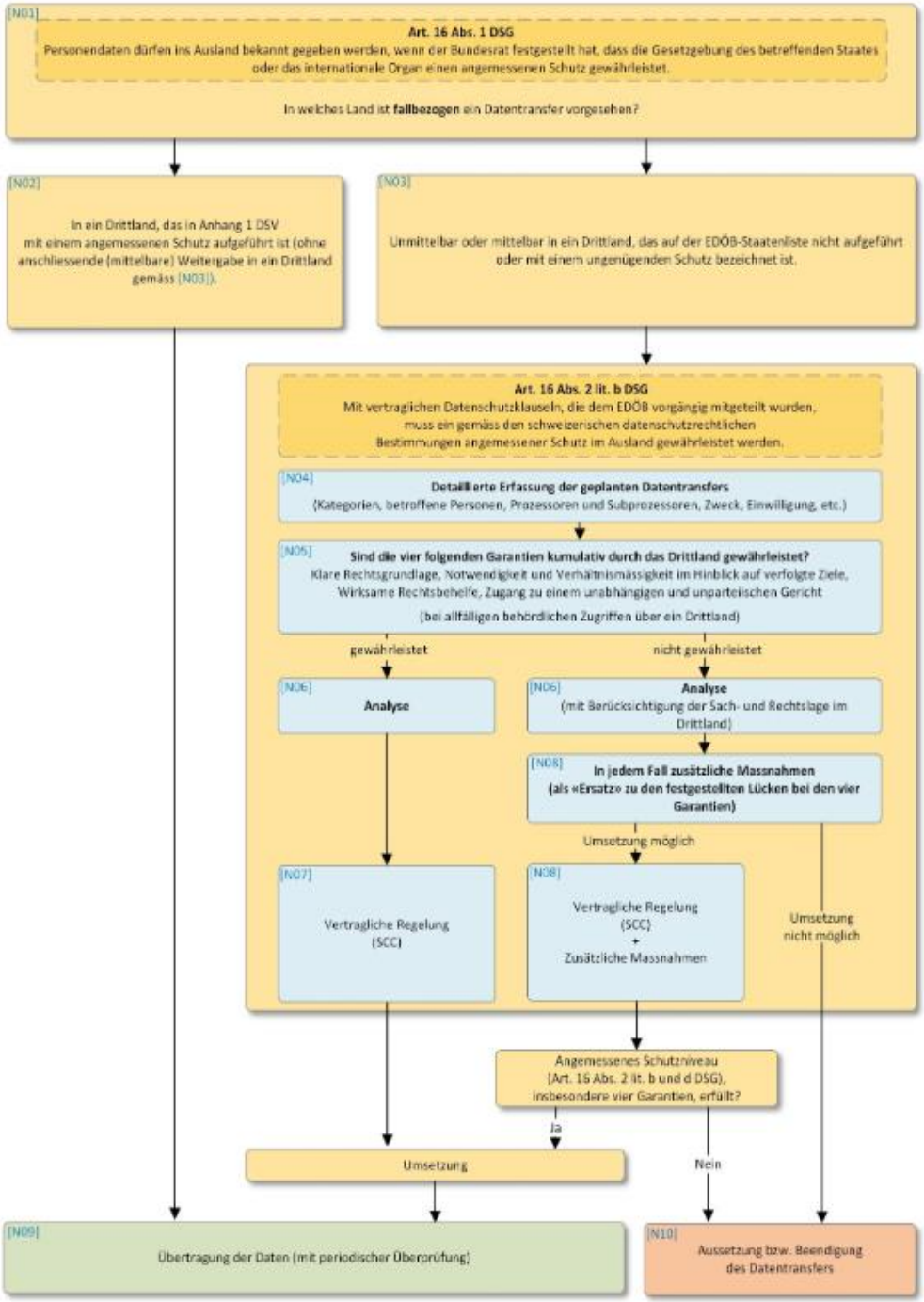
English (3.25 MB - ZIP) Herunterladen

4. JUNI 2021

Commission Implementing Decision on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725

English (314.16 KB - HTML) Herunterladen

https://commission.europa.eu/publications/publications-standard-contractual-clauses-sccs_de


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

MARCH 25, 2022

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

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

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

Erste Reaktionen

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

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

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

Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 30. März 2022

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

1. Ausgangslage

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

Namhafte Softwarehersteller wie Microsoft, Google, Amazon und

Kontroverse Auseinandersetzungen

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

Entscheidung der österreichischen Datenschutzbehörde vom 22. April 2022

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

Kontroverse Auseinandersetzungen

Microsoft 365: GRÜNE Luzern fordern Marschhalt und digitale Souveränität

Es braucht einen Marschhalt beim 28-Mio.-Projekt M365: Der Zugriff der amerikanischen Behörden auf vertrauliche Verwaltungsdaten und besonders schützenswerte Personendaten wie Gesundheits- und Steuerdaten der Luzerner*innen ist mit der Microsoft-Could künftig möglich. Recherchen zeigen: Sämtliche internen Sachverständigen und das Kantonsgericht, welche vor diesem Schritt warnten oder ihn gar als nicht legal bezeichneten, hat die Regierung ignoriert oder sogar freigestellt. Die GRÜNEN fordern in einem dringlichen Vorstoss einen sofortigen Marschhalt des Projekts – und endlich eine demokratische Debatte darüber, wie Luzern digital sicher und souverän bleibt und sich unser Kanton nicht noch stärker einem amerikanischen Grosskonzern ausliefert.

Der Luzerner Datenschutzbeauftragte sagt es deutlich: Luzern begeht mit seiner Daten-Auslagerung in die M365-Cloud einen Rechtsverstoss und liefert sich zudem einem einzigen amerikanischen Grosskonzern aus – dem Trump & Co. jederzeit Anweisungen erteilen können.

«Grundrechte wie das Recht auf digitale Selbstbestimmung der Luzerner*innen scheinen der Regierung egal – genauso wie die digitale Souveränität der Luzerner Verwaltung, denn sie liefert sich den Launen von Microsoft und Trump aus.»

Rahel Estermann, Kantonsrat GRÜNE Luzern

Appenzell Ausserrhoden

Beschlussentwurf
Departement Finanzen

17. Oktober 2024

Sitzungsdatum:
22. Oktober 2024

RRB-

Vgl. Protokoll-Nr.:

Im Ausstand von

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

G. Beschluss des Regierungsrates

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

2. Die Einführung von Microsoft 365 Cloud-Diensten in Kanton und Gemeinden wird, vorbehältlich der Genehmigung der Strategie-Ergänzung durch die Gemeinden, bewilligt.

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

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

Departement Finanzen

sign. 17. Oktober 2024

Hansueli Reutegger
Vorsteher Departement Finanzen

Microsoft-Amendment zu den SIK-Rahmenverträgen für die öffentlichen Verwaltungen

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.

Öffentliche Verwaltungen unter Amendment-Schutz des MS-RV mit DVS

Zur Einordnung:
Der DVS-Microsoft-Rahmenvertrag gewährt qualifizierenden Organisationen der öffentlichen Verwaltung vereinbarten Konditionen für EA/EAS/SCE-Beitritte mit Startdatum zwischen 01.05.2025 und 30.04.2028. Beitritte laufen grundsätzlich indirekt; der autorisierte Licensing Solution Partner (LSP) ist Hauptansprechpartner, und Preisanfragen sowie Bestellungen erfolgen über den LSP.

Zur Anerkennung:
Als Beitrittsunternehmen gelten ausschliesslich öffentliche Einrichtungen und Institutionen, die die definierten Kriterien erfüllen (öffentlich-rechtlicher Auftrag/Zweck, Non-Profit, kein Wettbewerb mit Privatwirtschaft). Für Grenzfälle gelten zusätzlich drei kumulative Prüffragen: Ertrag/Gewinn fliesst ausschliesslich an die öffentliche Hand, Steuerbefreiung von der direkten Bundessteuer, mindestens 50% Finanzierung durch die öffentliche Hand.

Greg Hernan
Geschäftsstelle Digitale Verwaltung Schweiz (DVS)
Direction opérationnelle Administration Numérique Suisse (ANS)

Haus der Kantone/ Maison des cantons
Speichergasse 6, 3003 Bern
Tel. +41 58 480 88 77
greg.hernan@gs-efd.admin.ch
www.digitale-verwaltung-schweiz.ch

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.

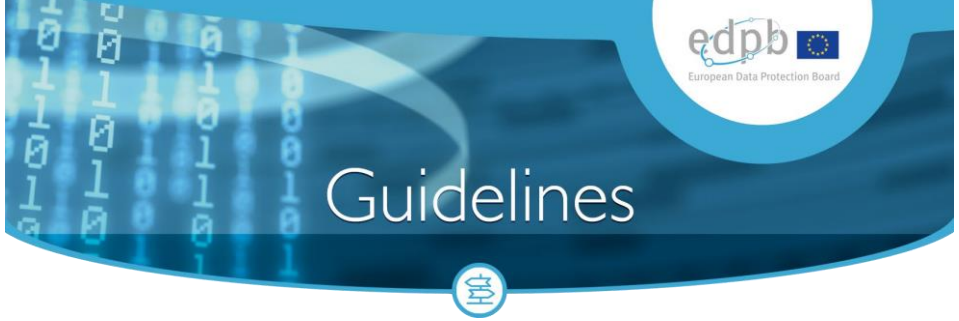
Schweizer Hotelbuchungsplattform verletzt die DSGVO-Informationspflicht in Österreich

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

Version 2.1

Adopted on 24 May 2023

Adopted

Table of Contents

09.09.2025	**2.400 €**	KVIKU SPAIN	ES	Unrechtmäßige Datenverarbeitung. »Details
09.09.2025	**3.600 €**	RIVER MADOS	ES	Unrechtmäßige Verarbeitung von Fingerabdrücken, unangemessene Datenschutz-Folgeabschätzung. »Details
08.09.2025	**325.000.000 €**	Google (Google LLC, Google Ireland Limited)	FR	Anzeige von Werbeanzeigen zwischen E-Mails in Postfächern ohne Einwilligung der Nutzer. »Details
08.09.2025	**7.287 €**	Dumitrescu Mihai-Ovidiu	RO	Speicherung von Cookies ohne Einholen einer Einwilligung. »Details
08.09.2025	**9.700 €**	Betreiber eines Studierendenwohnheims	BE	Unrechtmäßiger Betrieb von Überwachungskameras. »Details
08.09.2025	**1.200 €**	Privatperson	ES	Betrieb von Überwachungskameras, die Mitarbeiter-Ruhebereiche und öffentliche Räume erfassen. »Details
05.09.2025	**150.000.000 €**	Shein/Infinite Styles Services Co.	FR	Setzen von Cookies ohne Zustimmung der Nutzer. »Details
04.09.2025	**200.000 €**	DIGI SPAIN TELECOM	ES	Weitergabe von SIM-Karten an unbefugte Dritte. »Details
03.09.2025	**1.266 €**	Jason B., Pflegeheim-Direktor	UK	Verweigerung von Informationsanfragen. »Details

Zeige Bußgeld 41 bis 50 von 4379 Bußgeldern. 10 ▲ Bußgelder pro Seite.

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

Sanktionen nach schweizerischem Datenschutzrecht

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

8. Kapitel: Strafbestimmungen

Art. 60 Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten

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

a. die ihre Pflichten nach den Artikeln 19, 21 und 25–27 verletzen, indem sie vorsätzlich eine falsche oder unvollständige Auskunft erteilen;

b. die es vorsätzlich unterlassen:

1. die betroffene Person nach den Artikeln 19 Absatz 1 und 21 Absatz 1 zu informieren, oder

2. ihr die Angaben nach Artikel 19 Absatz 2 zu liefern.

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

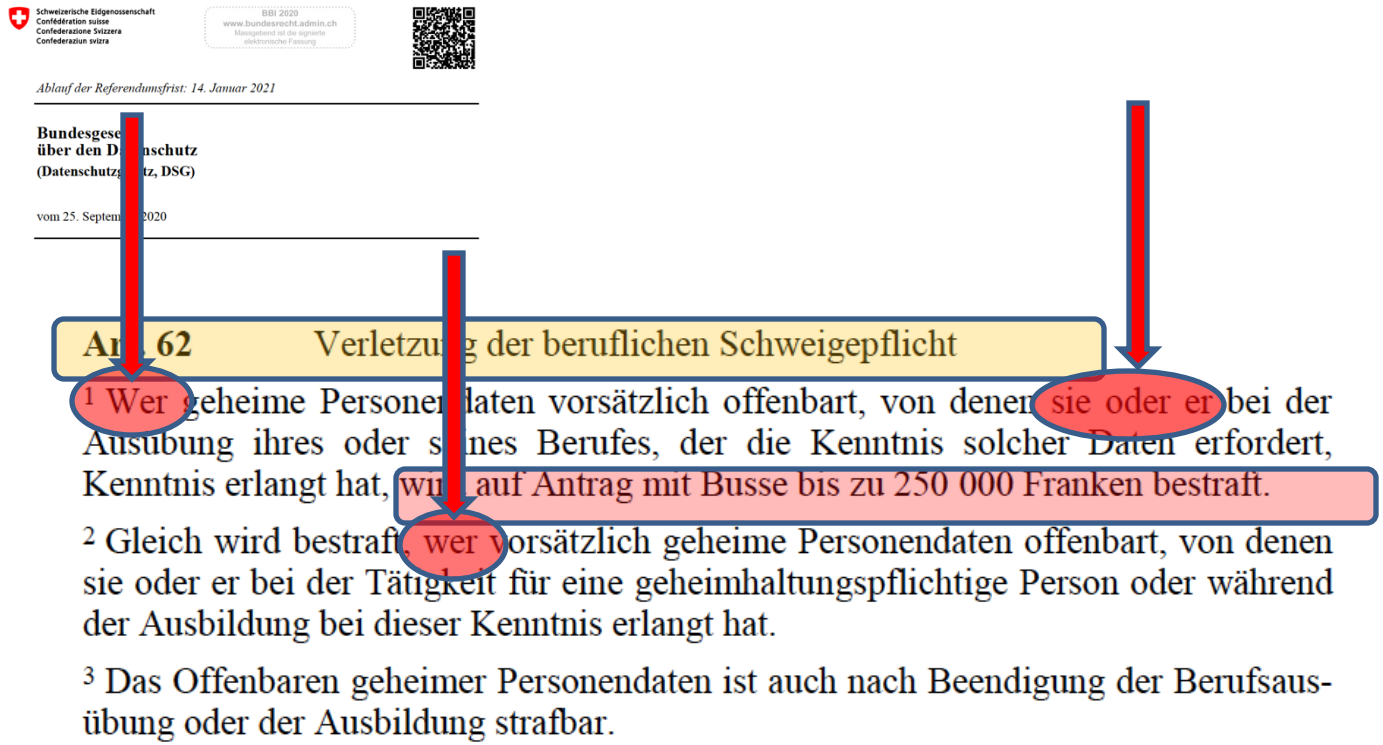
Art. 61 Verletzung von Sorgfaltspflichten

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

a. unter Verstoss gegen Artikel 16 Absätze 1 und 2 und ohne dass die Voraussetzungen nach Artikel 17 erfüllt sind, Personendaten ins Ausland bekanntgeben;

b. die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen nach Artikel 9 Absätze 1 und 2 erfüllt sind;

c. die Mindestanforderungen an die Datensicherheit, die der Bundesrat nach Artikel 8 Absatz 3 erlassen hat, nicht einhalten.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgese
über den D nschutz
(Datenschutz tz, DSG)

vom 25. Septem 2020

Ar 62 Verletzu g der beruflichen Schweigepflicht

[1] Wer geheime Personen laten vorsätzlich offenbart, von denen sie oder er bei der Ausübung ihres oder s nes Berufes, der die Kenntnis solcher Daten erfordert, Kenntnis erlangt hat, wi auf Antrag mit Busse bis zu 250 000 Franken bestraft.

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

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz über den Datenschutz (Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 63 Missachten von Verfügungen

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Ablauf der Referendumsfrist: 14. Januar 2021

Bundesgesetz
über den Datenschutz
(Datenschutzgesetz, DSG)

vom 25. September 2020

Art. 65 Zuständigkeit

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

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

Art. 66 Verfolgungsverjährung

Die Strafverfolgung verjährt nach fünf Jahren.

Die wichtigsten datenschutz- und datensicherheitsrechtlichen Aspekte für Unternehmen

Handlungsbedarf unter neuem CH-DSG

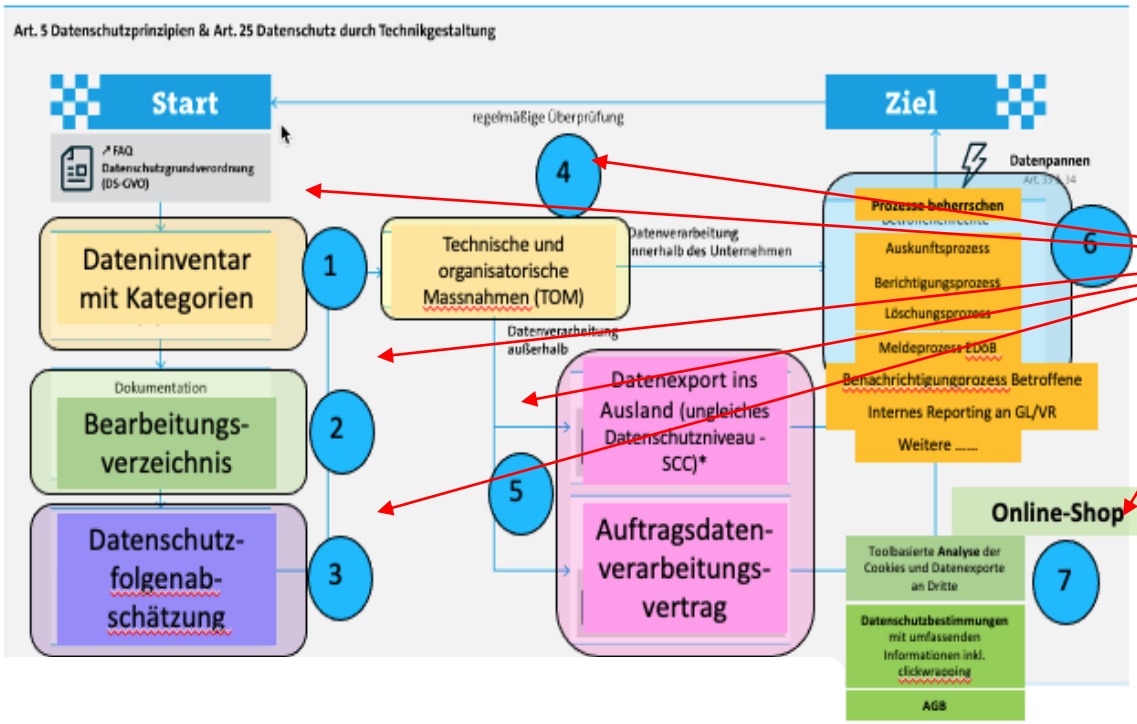
1. Inventar der Applikationen (interne und externe) und Ablagen erstellen
2. Personendaten erfassen
3. Datenschutzerklärungen auf den neuesten Stand bringen; prüfen ob alle Fälle abgedeckt sind, wo das Unternehmen Personendaten beschafft und bearbeitet.
4. Verzeichnis der Bearbeitungstätigkeiten erstellen (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

Schlussbericht und Empfehlungen

vom 25. April 2024

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)

in Sachen Xplain AG

aufgrund Ransomware-Vorfall

gemäss

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

Ausgangslage

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

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

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

IT-Infrastrukturen Xplain - Findings

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

IT-Infrastrukturen Xplain – Findings (2)

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

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

IT-Infrastrukturen Xplain – Findings (3)

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

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

IT-Infrastrukturen Xplain – Findings (4)

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

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

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

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

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

IT-Infrastrukturen Xplain – Findings (5)

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

- Die Support- und 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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

5. Empfehlungen

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

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

Empfehlungen:

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

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

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

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

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

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

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

Empfehlungen:

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

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

Rechtsmittelbelehrung:

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

Kanton Waadt kündigt Xplain-Vertrag

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

POLITIK & WIRTSCHAFT BESCHAFFUNG KANTON WAADT XPLAIN

Foto: zVg

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

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

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

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

Reputationsschaden als schwerwiegendste Unternehmensproblematik

Xplain ist verkauft

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

CHANNEL XPLAIN CHAPTERS GROUP ÜBERNAHME VERWALTUNG

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

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

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

Aktuelles aus unserer Kanzlei.

CAS Information-Security und Risk-Management

Verfasst am 29.05.2019
Fachhochschule Nordwest-Schweiz, FHNW in Basel

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

Grundsätze der Unternehmensführung
Coperate Governance und Complianc
Grundsätze von Datenschutz und neues Datenschutzrecht (DSGVO und E-DSG Schweiz)
Grundsätze von IT-Sicherheit
Schadensbegrenzung und Abwägung
››Weiterlesen

Datenschutz und Datensicherheit in der Arztpraxis

Verfasst am 16.05.2019

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

Fragen

Aufgabe 1

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

(max. 3 Grundsätze, was dem VR in Bezug auf die Einhaltung der Datenschutz- und Datensicherheits-Anforderungen 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)

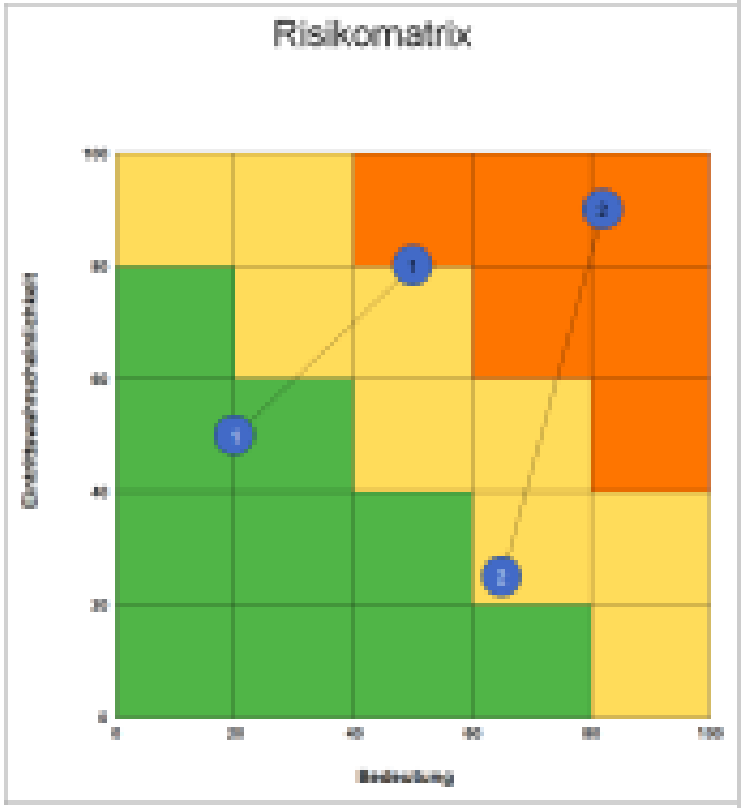
Im FaaS wird die XY AG u.a. auch Mitarbeiterdaten (Lohndaten, Sozialversicherungsdaten, Ferien- und Krankheitsabsenzen, vertrauensärztliche Atteste ihrer Mitarbeitenden) speichern.

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				
1					
2					
3					
4					
5					
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