GEWERBEVERBAND APPENZELL AUSSERRHODEN

KGVAI
KANTONALER GEWERBEVERBAND APPENZELL INNERRHODEN

CETRATUS

BURKHALTER RECHTSANWÄLTE
BERN / ZÜRICH

Datenschutz als strategisches Thema

Was ändert sich mit dem neuen DSG?

30. August 2023, Teufen

Dr. Matthias Amgwerd, Rechtsanwalt

Zürich, 30. August 2023

Inhalt

Inhalt

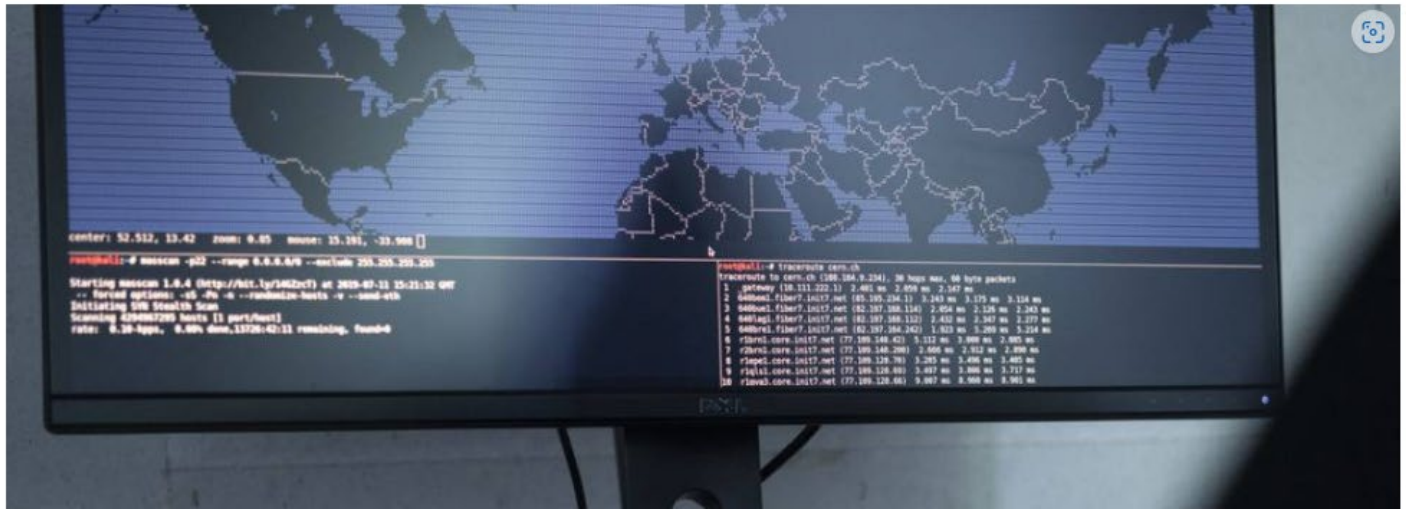
Keine Angst, es kann jeden treffen!

Appenzell

Hackerangriff auf Arztpraxis – hunderte Patientendaten im Darknet

Eine Appenzeller Arztpraxis ist vor einem Monat Opfer eines Hackerangriffs geworden. Nun sind sensible Patientendaten im Darknet aufgetaucht. Die Kantonspolizei Appenzell Innerrhoden bestätigt den Vorfall.

Jetzt mitdiskutieren

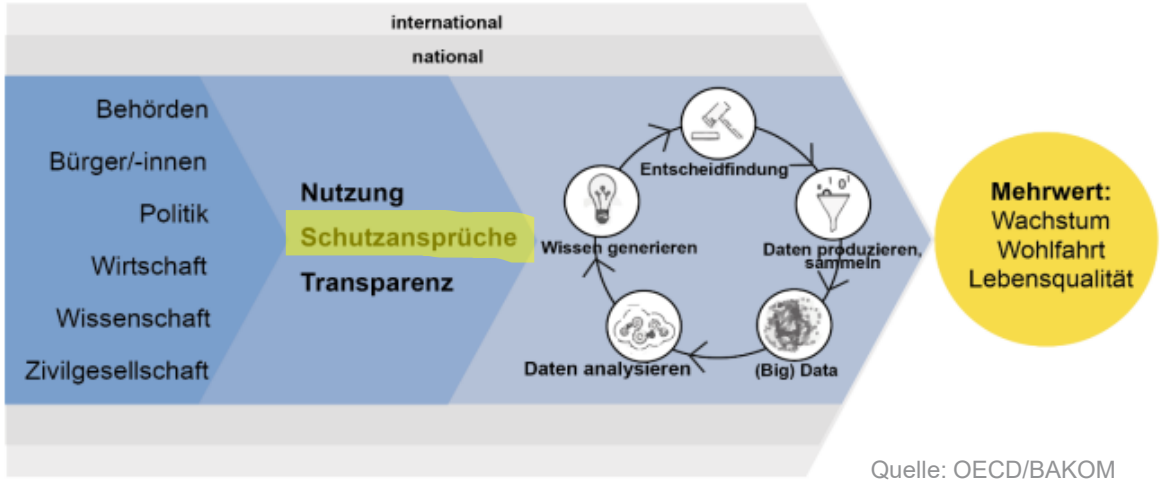


Datenpolitik

Datenpolitik als Aktionsfeld

- **Themen der Datenpolitik:** Dateninfrastruktur, Zugang zu digitalen Inhalten, Kontrolle über die eigenen Daten, Informationssicherheit etc.
- **Strategie «Digitale Schweiz»** vom BR 20. April 2016 verabschiedet
- Übergeordnete **Ziele** gemäss BR:
  - ➢ Förderung der **Standortattraktivität** für die **Wertschöpfung** durch Daten in der Schweiz
  - ➢ Schaffung von **modernen Rechtsgrundlagen** für den Umgang mit Daten
  - ➢ **Öffnung von Datenbeständen** als **Rohstoff** für die digitale Gesellschaft und Wirtschaft

Elemente einer kohärenten Datenpolitik



Quelle: OECD/BAKOM

„Datenpolitik ist die Summe der Massnahmen, die dazu führt, dass Mehrwert durch Daten realisiert werden kann."

(Arbeitsdefinition gemäss BAKOM)

Datenschutz: Grundlagen 1

- **Datenschutz ist Persönlichkeitsschutz – verfassungsrechtliches Grundrecht**

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.

Art. 1 Zweck

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

Art. 27 ff. Zivilgesetzbuch (ZGB) – Datenschutz als lex specialis

Es geht also (primär) nicht um den Schutz von Daten, sondern um den **Schutz von Personen** (Personendaten)

Im «Gegensatz» zu: Informationssicherheit (Unternehmensdaten) – ist aber Anliegen im Datenschutz

- Datenschutz und Informationssicherheit als **strategische Themen** (GL, VR) mit **zunehmender Bedeutung** (Regulierung, Sensibilisierung)
- **Risiko Management**, risikobasierter Ansatz
- Es gibt **kein Eigentum an Daten** («Ausnahme»: Geistiges Eigentum am Werk). Daten im **Konkurs**: neu Art. 242b SchKG

Datenschutz: Grundlagen 2

- **Rechtliche Grundlagen**
  - International: EMRK, Europarat Übereinkommen SEV 108, OECD
  - BV
  - Datenschutzgesetze (Bund und Kantone), Verordnungen

  - DSGVO und Co.

  - Empfehlungen Aufsichtsbehörden (EDÖB,…)
  - Rechtsprechung
- **Entwicklung**
  - USA, 1974, Privacy Act für Bundesbehörden – im privaten Bereich soll es der Wettbewerb regeln (!)
  - Hessen, 1970, erstes «modernes» Datenschutzgesetz
  - Europarat, 1981, Europäische Datenschutzkonvention
  - Bundesverfassungsgericht, 1983, Recht auf informationelle Selbstbestimmung als Grundrecht
  - Schweiz, 1993, Inkrafttreten DSG (Vorbereitungen ab 1971, aktuell in Revision), vorher bereits kantonale Erlasse

Verbindung zwischen Datenschutz und Informationssicherheit

Datenschutz

Der Datenschutz schützt Personendaten vor unzulässiger (unrechtmässiger) Bearbeitung

Persönlichkeitsschutz (betroffene Person)

auch durch Informationssicherheit

rechtlicher Ansatz

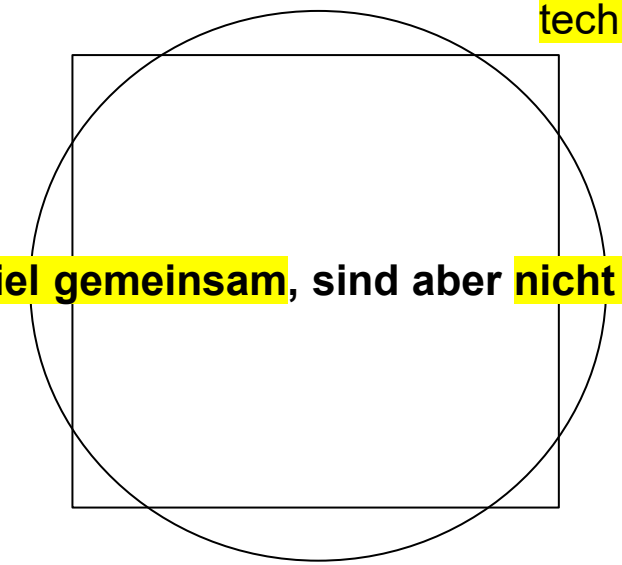
Informationssicherheit

Die Informationssicherheit (Datensicherheit) schützt Unternehmensdaten

«Unternehmensschutz»

auch Personendaten

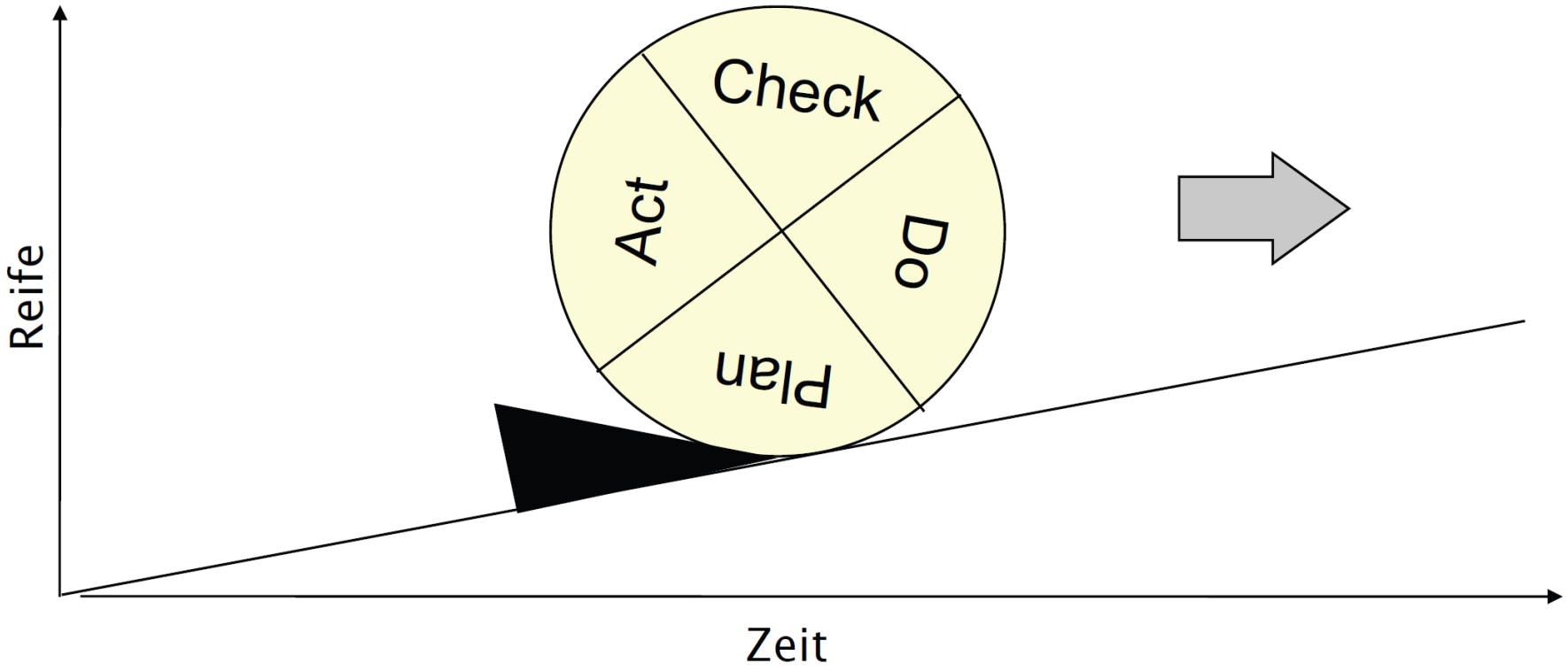
technischer und organisatorischer Ansatz



…haben viel gemeinsam, sind aber nicht das Gleiche.

Methodik

Datenschutz und Informationssicherheit sind kein Zustand, sondern ein Prozess (Regelkreis).
Das Ziel muss sein, immer besser zu werden.



Risikobasierter Ansatz (rechtlich, unternehmerisch)

Inhalt

Datenschutzgesetz (DSG): Geltungsbereich

Art. 2 Geltungsbereich

Revision!

[1] Dieses Gesetz gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch:

a. private Personen;

b. Bundesorgane.

[2] Es ist nicht anwendbar auf:

a. Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt;

b. Beratungen in den Eidgenössischen Räten und in den parlamentarischen Kommissionen;

c. hängige Zivilprozesse, Strafverfahren, Verfahren der internationalen Rechtshilfe sowie staats- und verwaltungsrechtliche Verfahren mit Ausnahme erstinstanzlicher Verwaltungsverfahren;

d. öffentliche Register des Privatrechtsverkehrs;

e. Personendaten, die das Internationale Komitee vom Roten Kreuz bearbeitet.

Datenschutzgesetz (DSG): Begriffe (Auszug)

Art. 3 Begriffe

Die folgenden Ausdrücke bedeuten:

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

b. *betroffene Personen:* natürliche oder juristische Personen, über die Daten bearbeitet werden;

c. *besonders schützenswerte Personendaten:* Daten über:
   1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
   2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
   3. Massnahmen der sozialen Hilfe,
   4. administrative oder strafrechtliche Verfolgungen und Sanktionen;

d. *Persönlichkeitsprofil:* eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt;

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

f. *Bekanntgeben:* das Zugänglichmachen von Personendaten wie das Einsichtgewähren, Weitergeben oder Veröffentlichen;

g. *Datensammlung:* jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind;

Revision!

Datenschutzgesetz (DSG): Allgemeine Grundsätze

- Die Grundsätze gemäss Art. 4, 5 und 7 müssen bei jeder Datenbearbeitung eingehalten werden
- Grundsätze (Revision!)
  - **Rechtmässige Datenbearbeitung** (nicht Täuschung, Arglist, Drohung)
  - **Zweckgebundenheit** (bei Datenerhebung), Zustimmung bei Zweckänderung
  - Vergewisserung über die **Richtigkeit**
  - **Verhältnismässigkeit**, d.h. soweit notwendig und geeignet, Eingriff so gering wie möglich
  - **Erkennbarkeit** bzgl. Erhebung und Zweck
  - **Datensicherheit** durch angemessene technische und organisatorische Masssnahmen Revision!
- Verstoss gegen diese Grundsätze: Verletzung der Persönlichkeit, Rechtfertigung gemäss Bundesgericht nicht ausgeschlossen, aber anspruchsvoll

Datenschutzgesetz (DSG): Weitere Regeln (1)

- **Datenübermittlung ins Ausland** (Art. 6)
  - Nicht erlaubt bei drohender Gefährdung der Persönlichkeit, namentlich fehlende „angemessene“ Gesetzgebung (vgl. Länderliste EDÖB)
  - Ersatz: Vertragliche Absicherung (Data-flow Agreement), Einwilligung und andere bestimmten Ausnahmen mit Auflagen (Anzeige)
- **Auskunft über Datenbearbeitung** (Art. 8-10)
  - Generelles, unverzichtbares Auskunftsrecht (ob)
  - Auskunftspflicht: Bestand, Herkunft, Zweck, Rechtsgrundlagen, Kategorien, Datenempfänger
  - In der Regel schriftlich und kostenlos
  - Einschränkung durch Gesetz oder überwiegende öffentliche oder private Interessen (Art. 9)
  - Medienprivileg, namentlich Quellenschutz (Art. 10)

Datenschutzgesetz (DSG): Weitere Regeln (2)

- **Datenbearbeitung durch Dritte** (Art. 10a)
  - gestützt auf Gesetz oder Vertrag (keine Geheimhaltungspflichten)
  - gemäss ursprünglichem Zweck
- **Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen** (Art. 14) **Revision!**
  - Ausnahme: Gesetz, unverhältnismässiger Aufwand
  - Einschränkung durch Gesetz oder überwiegende öffentliche oder private Interessen
- **Zertifizierungsverfahren** (Art.11)
  - zur Verbesserung Datenschutz und Datensicherheit
  - durch anerkannte unabhängige Zertifizierungsstellen (ISO)
- **Register der Datensammlung** (Art. 11a)
  - Anmeldung bei EDÖB vor Eröffnung
  - Bund allgemeine Pflicht, Private bei (a) besonders schützenswerten Daten und Persönlichkeitsprofilen oder (b) regelmässige Bekanntgabe von Daten an Dritte **Revision!**
  - Ausnahmen: gesetzliche Verpflichtung, Medienprivileg, Ernennung Datenschutzverantwortlicher, Zertifizierung

Datenschutzgesetz (DSG): Weitere Regeln (3)

- **Vorgehen bei Persönlichkeitsverletzungen**
  - Persönlichkeitsverletzungen (Art. 12)
  - Rechtfertigung der Verletzung (Art. 13)
  - Rechtsansprüche (Art. 15)

    Klage auf Unterlassung, Beseitigung, Feststellung, Mitteilung, Schadenersatz, Genugtuung, Herausgabe des Gewinns

    Zivilverfahren

- **Strafbestimmungen**
  - Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten (Art. 34)
  - Verletzung der beruflichen Schweigepflicht (Art. 35)
  - „Zahnloses“ Sanktionssystem: Busse maximal 10‘000 Franken (Art. 106 StPO)

Revision!

Datenschutz (DSG): «Aufsichtsbehörde» EDÖB

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Der Beauftragte

Adrian Lobsiger

Adrian Lobsiger, geb. am 27.12.1959, hat nach seinem Studium an den Universitäten in Bern und Basel ein Masterstudium in Europarecht in Exeter (GB) absolviert. 1992 trat der promovierte Jurist in den Bereich Internationales Privatrecht des Bundesamtes für Justiz (BJ) ein, bevor er 1995 ins Bundesamt für Polizei (fedpol) wechselte, wo er zuletzt als stellvertretender Direktor amtierte. Als Chef der Stabsabteilung und des dazugehörigen Dienstes für Recht und Datenschutz war er für die rechtskonforme Bearbeitung von Personendaten im Verkehr mit in- und ausländischen Behörden verantwortlich. In den Jahren 2000 bis 2005 gründete und leitete er nebenamtlich das Nachdiplomstudium zur Bekämpfung der Wirtschaftskriminalität sowie das Kompetenzzentrum für Forensik und Wirtschaftskriminalistik an der Hochschule Luzern.

Adrian Lobsiger wurde im November 2015 vom Bundesrat gewählt und im März 2016 vom Parlament bestätigt. Er ist seit Juni 2016 im Amt.

Datenschutz

Vgl. auch Abschnitt 5 DSG

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat im Bereich Datenschutz insbesondere folgende Aufgaben:

- Er berät Bürgerinnen und Bürger, Unternehmen und private Organisationen,
- er beaufsichtigt die Datenbearbeitungen von Unternehmen und privaten Organisationen,
- er berät die Bundesverwaltung und die bundesnahen Betriebe,
- er beaufsichtigt die Datenbearbeitungen der Bundesverwaltung und der bundesnahen Betriebe (u.a. SBB, Post, Swisscom).
- Der EDÖB nimmt Stellung zu Rechtsetzungsprojekten des Bundes,
- er tauscht sich mit in- und ausländischen Datenschutzbehörden aus und arbeitet fallweise mit ihnen zusammen,
- er sensibilisiert und informiert die Öffentlichkeit,
- er führt und veröffentlicht das Register der Datensammlungen.

Wichtig:
Datenbearbeitungen der kommunalen und kantonalen Behörden fallen in den Zuständigkeitsbereich der Datenschutzstellen der Kantone bzw. Gemeinden.

Um seine Aufgaben zu erfüllen, kann der EDÖB von sich aus oder auf Meldung Dritter Sachverhalte näher abklären und aufgrund dieser Abklärungen Empfehlungen erlassen.

Der EDÖB hat im Privatbereich vorab beratende Funktionen. Insbesondere erläutert er das Datenschutzgesetz und die Vollzugsverordnungen, bietet Anleitung und Hilfe bei der Anmeldung von Datensammlungen und Datenübermittlungen ins Ausland und bei der Gewährung/Ausübung des Auskunftsrechts. Er berät sowohl in rechtlichen Fragen als auch bei technischen Aspekten der Datensicherung.

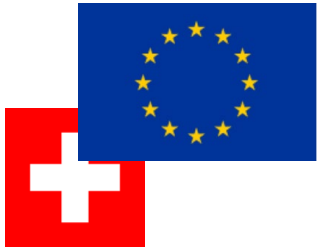
Inhalt

EU Datenschutz-Grundverordnung (DSGVO)

Datenschutz (DSGVO): Überblick

- **Verordnung:** direkte Anwendbarkeit für EU/EWR
- „In Kraft“ seit 25. Mai 2018
- Umsetzung **digitaler Binnen-markt**
- **Extraterritorialer Geltungs-bereich:** Marktortprinzip – auch für Schweizer Unternehmen mit EU-Bezug relevant
- Erhebliche **Verschärfung** von Rechten, Pflichten, Kontrollen, Kompetenzen und Sanktionen
- Relevant für aktuelle **DSG-Revision** (Angemessenheitsentscheid EU-Kommission)

Datenschutz (DSGVO): Welche Schweizer Unternehmen sind betroffen?



- Art. 3 DSGVO
- **Kriterium der Niederlassung:** Unternehmen (Verantwortlicher) oder beauftragter Dritter (Auftragsbearbeiter) im Rahmen der Tätigkeit einer Niederlassung innerhalb der EU, unabhängig davon ob die Verarbeitung tatsächlich in der EU stattfindet.
- **Kriterium des Zielmarktes:** Datenverarbeitung durch Verantwortlicher oder Auftragsbearbeiter ohne Niederlassung in der EU bezieht sich auf Personen, die sich in der EU befinden und sofern
  a. diesen Personen in der EU Waren oder Dienstleistungen entgeltlich oder unentgeltlich angeboten werden oder
  b. Das Verhalten dieser Personen in der EU beobachtet wird.
- Zugang Website genügt nicht, Angebote in Euro ist u.a. Indiz
- Leitlinien 3/2018 zum räumlichen Anwendungsbereich der DSGVO (Artikel 3), Version 2.0, 12. November 2019

Datenschutz (DSGVO): Verschärfung bestehender Regeln (1)

- Ersetzt bisherige Richtlinie (nicht direkt anwendbar)
- Ähnliche **Grundsätze der Datenverarbeitung** (Art. 5):
  - Rechtmässigkeit
  - Treu und Glauben
  - Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Speicherbegrenzung
  - Integrität und Vertraulichkeit
  - Rechenschaftspflicht

Datenschutz (DSGVO): Verschärfung bestehender Regeln (2)

- Strenge Umsetzung des **Prinzips der Rechtmässigkeit** (Art. 6 ff.).
  - ausdrückliche Einwilligung der betroffenen Person
  - für Abschluss oder Erfüllung eines Vertrags erforderlich
  - für Erfüllung einer gesetzlichen Pflicht erforderlich
  - zur Wahrung überwiegender berechtigter Interessen
- Ausgebaute **Rechte und Pflichten**:
  - Informationspflichten (Art. 13 und 14)
  - Auskunftsrechte (Art. 15)
  - Recht auf Berichtigung, Löschung und Einschränkung der Bearbeitung (Art. 16-18)
  - Recht auf Datenübertragbarkeit (Art. 20)
  - Widerspruchsrechte (Art. 21)

Datenschutz (DSGVO): Verschärfung bestehender Regeln (3)

- **Weitere Regeln**
  - Datenschutz durch Technikgestaltung (Protection by Design) und durch datenschutzfreundliche Voreinstellungen (Protection by Default) (Art. 25)
  - Verzeichnis der Verarbeitungstätigkeiten (Dokumentationspflicht, Art. 30)
  - Sicherheit der Verarbeitung (Art. 32)
  - Datenschutz-Folgeabschätzung (Art. 35 f.)
  - Ernennung eine Datenschutzbeauftragten (Art. 37-39) und eines Vertreters in der EU (Art. 27)
  - Verhaltensregeln durch Verbände (Art. 40 f.) und Zertifizierung (Art. 42 f.)
  - bei Datenschutzverletzungen Meldepflicht gegenüber Aufsichtsbehörden (Art. 33) und gegenüber betroffenen Personen (Art. 34)
  - umfassende Untersuchungsbefugnisse, hohe Sanktionen bei Verstössen möglich: bis 4% Jahresumsatz bzw. 20 Mio. Euro (Art. 83)
  - Amtshilfe zwischen EU/EWR-Staaten (Art. 61) und zu Drittstaaten (Art. 50)
  - Schadenersatz (Art. 82)
- **Fazit:** Die DSGVO führt zu einer Verbesserung der Betroffenen-Rechte und zugleich zu einer erheblichen Steigerung des Aufwands für Unternehmen sowie Behörden und zumindest vorübergehend auch zu Rechtsunsicherheit.

Inhalt

Datenschutz: Revision DSG – Ablauf (1)

- Evaluationsbericht 9. Dezember 2011
- Bericht Begleitgruppe 1. April 2015
- 21. Dezember 2016 Vernehmlassung
- Botschaft vom 15. September 2017 zur „Totalrevision“ DSG

  Ziele (Bundesrat):

  - Datenschutz stärken (Verbesserung Transparenz und Kontrollmöglichkeiten)
  - Erhöhung des Verantwortungsbewusstsein der für die Verarbeitung Verantwortlichen
  - Verbesserung der Aufsicht
  - Übernahme Schengen-Acquis
  - Annäherung an DSGVO: Angemessenheitsentscheid
  - Übernahme eines Protokolls zum Europarat Übereinkommen SEV 108

  Zahlreiche Änderungen und Verbesserungen gegenüber dem Vorentwurf: im Ergebnis weniger „autonomer Nachvollzug“ (so weit wie nötig, so wenig wie möglich)

Datenschutz: Revision DSG - Ablauf (2)

- Parlamentarische Beratung Dezember 2016 bis Oktober 2020
  - Knackpunkte:
    - Profiling
    - Informationspflichten
    - Datenportabilität
    - Sanktionssystem
    - …
  - Staatspolitische Kommissionen, National-/Ständerat, Einigungskonferenz
  - Vorlage drohte zu scheitern – EU-Angemessenheitsentscheid rettete sie

- Aktuell: Anpassung Ausführungsverordnungen
- Inkrafttreten per 1. September 2023 – keine Übergangsregelung!

Datenschutz: Revision DSG – Grundzüge

- Die wesentlichen Grundsätze bleiben unverändert – keine Revolution!
- Anhebung des Datenschutzes auf „DSGVO-Niveau“ (Angemessenheit)
- Erhöhung der Transparenz
- Stärkung der Betroffenenrechte
- Neue und erweiterte Pflichten
- Kein befürchteter „Swiss-Finish“
- Erhebliche Stärkung der Aufsicht bzw. der Kompetenzen des EDÖB
- Verschärfung Sanktionssystem
- Ausbau und internationalen und interkantonalen Amtshilfe

Datenschutz: Revision DSG – wichtige Neuerungen (1)

- Auswirkungsprinzip (Extrateritorialität) (Art. 3)
- Daten über juristische Personen nicht mehr erfasst; Verweis Art. 28 ZGB, UWG etc.
- Rollenbezeichnung: Verantwortlicher (controller) und Auftragsbearbeiter (processor)
- Unterauftragsbearbeiter nur mit Zustimmung des Verantwortlichen (Art. 9 Abs. 3)
- Daten zur ethnischen Herkunft sowie genetische wie auch biometrische Daten besonders schützenswert (Art. 5 Bst. c)
- Allgemeine und umfassende Informationspflicht bei Beschaffung von Personendaten (Art. 19) und Ausnahmen (Art. 20)
- Vernichtung oder Anonymisierung bei Zweckerfüllung (Art. 6 Abs. 4)
- Datenschutz durch Technik (privacy by design) und datenschutzfreundlich Voreinstellungen (privacy by default) (Art. 7)

Datenschutz: Revision DSG – wichtige Neuerungen (2)

- Ausdrückliche Einwilligung bei besonders schützenswerten Personendaten und Profiling mit hohem Risiko für Persönlichkeit und Grundrechte (Art. 6 Abs. 7) – aber nur für Rechtfertigung
- Pflicht zur Führung eines Verzeichnisses über die Datenbearbeitungs-tätigkeiten (Art. 12) – Möglichkeit der Erleichterungen für KMU
- Verhaltenskodex (Art. 11) und Zertifizierung (Art. 13)
- Pflicht zur aktiven Überwälzung der Datenschutzverpflichtungen auf den Auftragsbearbeiter (Art. 9) – (schriftliche) Datenbearbeitungsvereinbarung
- Pflicht zur Datenschutz-Folgenabschätzung bei hohem Risiko für Persönlichkeit und Grundrechte (Art. 22)
- Meldepflicht bei Verletzung der Datensicherheit bei hohem Risiko für Persönlichkeit und Grundrechte (Art. 24)
- Ausweitung der beruflichen Schweigepflicht auf alle geheimen Personendaten (Art. 62) – „Berufsgeheimnis für jedermann“

Datenschutz: Revision DSG – wichtige Neuerungen (3)

- Recht auf (beschränkte) Datenherausgabe und -übertragung (Datenportabilität) (Art. 28)
- Stärkung der Kompetenzen EDÖB (Art. 49 ff.)
  - Untersuchungen von Amtes wegen oder auf Anzeige hin
  - Verfügungskompetenz
- Verschärfung der Sanktionen (Art. 60 ff.)
  - Neue Straftatbestände (z.B. Verletzung von Sorgfaltspflichten, Missachtung von Verfügungen)
  - Voraussetzung: Vorsatz, Anzeige
  - strafbar bleibt der Einzelne (nicht Unternehmen), aber auch Management/VR!
  - Verfolgung nach wie vor durch Kantone (EDÖB Recht auf Anzeige und Privatklägerschaft)
  - Bussen bis 250‘000 Franken

Inhalt

Fazit: Was ändert sich mit dem neuen DSG?

- Kein Systemwechsel – aber überall wird die Schraube angezogen!
- Was sich (dramatisch) verändert hat und weiter verändern wird, ist die Wahrnehmung von und die Sensibilisierung für Datenschutz und Informationssicherheit.
- Die Regulierung wird weiter zunehmen, namentlich auch im Bereich der Informationssicherheit.

  Beispiel Medizinprodukteverordnung:

  Art. 74 Cybersicherheit

  [1] Gesundheitseinrichtungen treffen alle technischen und organisatorischen Massnahmen, die nach dem Stand der Technik notwendig sind, um bei netzwerkfähigen Produkten den Schutz vor elektronischen Angriffen und Zugriffen sicherzustellen.

  [2] Spitäler identifizieren, bewerten und dokumentieren die Massnahmen nach Absatz 1 gemäss den Grundsätzen eines Risikomanagementsystems. Dieses System ist integraler Bestandteil des Qualitätsmanagementsystems der Spitäler.

  Selbstregulierung als Alternative?

- Datenschutz/Informationssicherheit sind ein strategisches Thema im Rahmen des Risikomanagements
  - Haftung, auch Organe gegenüber Gesellschaft (Art. 717 Abs. 1 OR)
  - Reputation
  - Sanktionen
  - Business Continuity

Inhalt

Praxistipps Datenschutz

- Datenschutz und Informationssicherheit sind strategische Themen (Governance) und im Verantwortungsbereich von Geschäftsleitung und Verwaltungsrat. Wir empfehlen einen risikobasierten Ansatz. Verantwortlichkeiten klären!
- Jedem Unternehmen sollte bewusst sein, welche Personendaten zu welchem Zweck bearbeitet werden und wie diese geschützt werden.
- Unternehmen sollten sich bei sämtlichen Datenbearbeitungen über deren Rechtmässigkeit im Klaren sein. Beschäftigen Sie sich auch mit den Ausnahmen von Rechten und Pflichten.
- Eine praktikable Umsetzung der Informationspflicht erfolgt in AGB und Datenschutzerklärung (Website), letztere mit hoher Aussenwirkung.
- Die Datenbearbeitung und der Datenschutz sollten angemessen dokumentiert und aktualisiert sein.
- Der Datenschutz sollte – wo nötig – genügend vertraglich abgesichert sein.
- Bei jedem Projekt sollte eine „kleine“ Datenschutz-Folgenabschätzung gemacht werden.
- Jedes Unternehmen sollte seine Mitarbeitenden im Bereich Datenschutz und -sicherheit schulen und sensibilisieren.
- Die Prozesse zu Datenschutz und -sicherheit sollten bekannt und eingespielt sein.

…und was ist nun zu tun?

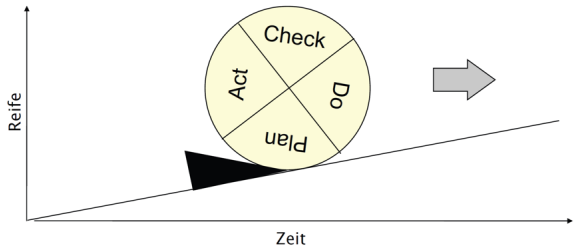
- **Nehmen Sie Datenschutz und Informationssicherheit auf die Agenda – Regeln Sie die Verantwortung**

- **Informieren Sie sich weiter**
  - Chancen und Risiken
  - Merkblatt und Vorlagen

SCHWEIZERISCHE Gewerbezeitung
DIE ZEITUNG FÜR KMU

- **Legen Sie mit der Umsetzung los**

- **Ziehen Sie – wo nötig – Hilfe bei**



CHECKLISTE FÜR KMU

- Datenbearbeitungsverzeichnis erstellen
- GAP-Analyse durchführen (Vergleich Soll-/Istzustand)
- Sensibilisierung Mitarbeiter bezüglich des Themas «Datenschutz»
- Datenschutzerklärung überprüfen und ggf. anpassen
- Datenschutzrichtlinien erstellen, Datenschutzverträge (Auftrags-bearbeitung, Bearbeitung im Ausland) aktualisieren
- Verantwortlichkeiten klären und Prozesse definieren
- Restrisiken bewusst in Kauf nehmen

Die Checkliste ist nicht abschliessend und kann demnach keine Rechtsberatung ersetzen.

Besten Dank!

Kontakt:
Matthias Amgwerd, 079 686 05 16, amgwerd@drpb.ch
www.drpb.ch www.cetratus.ch