VISCHER

Das neue Schweizer Datenschutzgesetz:

Eine Anleitung für jene, die die DSGVO schon eingeführt haben

David Rosenthal, Partner, VISCHER AG
22. Juni 2023

Fünf Jahre nach der DSGVO …

- Ab 1. September 2023 ein neues **Datenschutzgesetz**
  - https://www.fedlex.admin.ch/eli/oc/2022/491/de
  - Keine (relevante) Übergangsfrist
- Ähnlich wie die **EU DSGVO**, aber (zum Glück) **keine Kopie**
  - Pragmatischer und weniger formalistisch als das EU-Recht
  - Nur in wenigen Bereichen strenger als DSGVO
  - Was bisher an Bearbeitungen erlaubt war, bleibt es meist
  - Neue Pflichten im Bereich Governance, Dokumentation, Aufsicht
  - **Aber:** Persönliche **Strafbarkeit** bei bestimmten Verletzungen

Was ändert sich? Was ist neu?

Ausführliche kostenlose Kommentierung: https://bit.ly/3kUfzqu

1. Ausgebaute Pflicht zur **Datenschutzerklärung***
2. Pflicht für ein **Verzeichnis der Datenbearbeitungen**
3. Leicht strengere Vorgaben für **Auftragsbearbeitungen***
4. Pflicht zur **Datenschutz-Folgenabschätzung** in heiklen Fällen
5. Pflicht zur **Meldung von Sicherheitsverstössen** an EDÖB
6. Anpassung des **Auskunfts-* und Korrekturrechts**
7. Neues Recht auf **Datenportabilität** für Kunden
8. Regelung zu **automatisierten Einzelentscheiden***
9. Anpassung diverser **Begrifflichkeiten**
10. Aufsichtsinstrumente und ***Strafbarkeit ausgebaut**

Die Grundsätze verändern sich nicht!

Welche Bearbeitungen sind zulässig?

Keine Anpassungen

DSGVO

- Bearbeitungsgrundsätze
  - Transparenz, Zweckbindung, Fairness, Datenminimierung, begrenzte Speicherfristen, Datenrichtigkeit, Datensicherheit
- Rechtsgrund erforderlich
  - Vertrag, gesetzliche Verpflichtung, Einwilligung, berechtigtes Interesse, etc.

Revidiertes DSG

- Dieselben Bearbeitungsgrundsätze
- Aber: Im Normalfall ist kein Rechtsgrund erforderlich
  - Nur dann, wenn Grundsätze *nicht* eingehalten werden, Dritten bes. schützenswerte Daten offenbart werden oder die betroffene Person der Bearbeitung widerspricht
  - DSG weniger eingeschränkt bei den Rechtfertigungsgründen für die Bearbeitung sensitiver Daten

Wann ist eine Einwilligung gültig?

Keine Anpassungen

DSGVO

- Einwilligung nur nach vorgängiger Information, für den bestimmten Fall, freiwillig und unmissverständlich
- Keine vorangekreuzten Kästchen
- Koppelungsverbot (mit Vertrag), ausser wo für Vertragserfüllung nötig
- Zwingender Hinweis auf das Recht auf Widerruf
- Widerruf ist jederzeit; i.d.R. keine Berufung auf berechtigte Interessen

Revidiertes DSG

- Freiwillig auf informierter Basis
- vorangekreuzte Kästchen zulässig, sofern dem Formular als solchen mittels Knopfdruck zugestimmt wird
- Abgabe im Rahmen eines Vertrags zulässig, sofern sachlicher Bezug
- Hinweis auf Widerruf nicht nötig
- Widerruf kann eingeschränkt werden (z.B. bei geschäftlichen Nutzungen)

Geltungsbereich

Anwendbarkeit prüfen

DSGVO

- Verarbeitung von Daten einer identifizierten oder identifizierbaren Person
- Automatische Verarbeitungen; manuelle nur bei Datensammlungen
- Haushaltsausnahme (≠ beruflich)
- Anwendung ausserhalb EWR, wenn
  - Targeting von Personen im EWR betr. Waren/Dienstleistungen
  - Verhaltensbeobachtung im EWR

Revidiertes DSG

- Dieselbe Definition (Personendaten)
  - Nicht mehr: juristische Personen
- Sämtliche automatischen und manuellen Bearbeitungen erfasst
- Ausnahmen für persönliche Zwecke (privat und beruflich)
- Keine Anwendung in Rechtsverfahren
- Extraterritorialität sofern Aktivitäten, Verantwortliche, Auftragsbearbeiter oder betroffene Personen in Schweiz

"Bundesorgane"

Anwendbarkeit prüfen

- Private Institutionen können auch **"Bundesorgane"** sein
- Wer **öffentliche Aufgabe des Bundes** erfüllt
  - Krankenversicherungen in der Grundversicherung
  - Pensionskassen im obligatorischen Bereich
- In diesen Fällen gelten für sie **strengere Regeln**
  - https://www.vischer.com/know-how/blog/pensionskassen-diese-dsg-sonderpflichten-gelten-fuer-sie-40126/
  - Pflicht zur Rechtsgrundlage
  - Pflicht zum Bearbeitungsreglement, ROPA
  - Pflicht zum "Datenschutzberater"


VISCHER

Dienstleistungen Team Know-how Karriere

Start › Know-how

Pensionskassen: Diese DSG-Sonderpflichten gelten für sie.

1. Juni 2023

Teilen:

- Pensionskassen sind im Obligatorium "Bundesorgane"
- Das revDSG sieht daher zusätzliche Pflichten für sie vor
- Ein "Datenschutzberater" muss ernannt werden

Mit dem revidierten Datenschutzgesetz (**revDSG**) kommen auf viele Betriebe am 1. September 2023 neue Herausforderungen zu. Für eine Kategorie von Organisationen gelten jedoch erschwerte Bedingungen: Betriebe, die mit öffentlichen Aufgaben betraut sind. Dazu gehören Versicherer in der obligatorischen Krankenpflegeversicherung (**OKP**) und Unfallversicherung (**UVG**), aber beispielsweise auch (im Obligatorium tätige) Pensionskassen-Stiftungen (**PK**) und Verbandsausgleichskassen (**VAK**). Sie alle setzen öffentliches Recht wie namentlich das KVG, UVG, BVG oder AHVG um und unterliegen daher im Datenschutzrecht den Regeln

Informationspflichten

DSE anpassen

DSGVO

- Erhebung von Personendaten löst Informationspflicht gegenüber der betroffenen Person aus (Mitteilung der Datenschutzerklärung, "DSE")
- DSGVO 13 ff. definiert Mindestinhalt der Datenschutzerklärung
- Gilt auch, wenn Personendaten via Dritte erhoben werden
- Nur sehr wenige Ausnahmen

Revidiertes DSG

- Ähnliche Pflicht, kein abschliessender Katalog an Informationen
- Mindestinhalt ist kürzer; Infos gem. DSGVO 13(2) nur ausnahmsweise
- Mehr Ausnahmen (z.B. für gesetzlich geregelte Datenbearbeitungen)
- **Aber:** Anzugeben sind alle Länder, in welche Personendaten übertragen werden (inkl. Grundlage für Exporte in unsichere Länder)

Busse!

Informationspflichten

[2] Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

a. die Identität und die Kontaktdaten des Verantwortlichen;

b. den Bearbeitungszweck;

c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

Art. 19 Abs. 2 revDSG

Art. 20 Abs. 3 revDSG

[3] Der Verantwortliche kann die Mitteilung der Informationen in den folgenden Fällen einschränken, aufschieben oder darauf verzichten:

a. Überwiegende Interessen Dritter erfordern die Massnahme.

b. Die Information vereitelt den Zweck der Bearbeitung.

c. Der Verantwortliche ist eine private Person und die folgenden Voraussetzungen sind erfüllt:

1. Überwiegende Interessen des Verantwortlichen erfordern die Massnahme.

2. Der Verantwortliche gibt die Personendaten nicht Dritten bekannt.

Datenschutzerklärung

plus Verweise auf DSGVO ergänzen, ggf. Anpassungen bei den Betroffenenrechten, Datenschutzberater im Sinne des Gesetzes und Vertreter nennen

Gehen Personendaten ins Ausland?

- ☐ Nein, das ist nicht geplant.
- ☐ Ja, das ist möglich, in den **EWR**, aber ausnahmsweise in jedes Land der Welt (denkbar insb. bei Online-Services, die wir nutzen). Ist das ein Land ohne genügenden Datenschutz, schliessen wir insb. die EU-Standardvertragsklauseln ab, können uns aber fallweise auch auf Einwilligungen abstützen oder Daten ins Ausland geben, weil es für die Abwicklung eines Vertrags nötig ist, wo es um von Ihnen veröffentlichte Daten geht oder es für Rechtsverfahren im Ausland nötig ist.

8. Gelangen Ihre Personendaten auch ins Ausland?

Wie in Ziff. 7 erläutert, geben wir Daten auch anderen Stellen bekannt. Diese befinden sich nicht nur in der Schweiz. Ihre Daten können daher sowohl in Europa als auch in [Land] bearbeitet werden; in Ausnahmefällen aber in jedem Land der Welt.

Befindet sich ein Empfänger in einem Land ohne angemessenen gesetzlichen Datenschutz, verpflichten wir den Empfänger vertraglich zur Einhaltung des anwendbaren Datenschutzes (dazu verwenden wir die revidierten Standardvertragsklauseln der Europäischen Kommission, die hier: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj? abrufbar sind), soweit er nicht bereits einem gesetzlich anerkannten Regelwerk zur Sicherstellung des Datenschutzes unterliegt und wir uns nicht auf eine Ausnahmebestimmung stützen können. Eine Ausnahme kann namentlich bei Rechtsverfahren im Ausland gelten, aber auch in Fällen überwiegender öffentlicher Interessen oder wenn eine Vertragsabwicklung eine solche Bekanntgabe erfordert, wenn Sie eingewilligt haben oder wenn es sich um von Ihnen allgemein zugänglich gemachte Daten handelt, deren Bearbeitung Sie nicht widersprochen haben.

https://www.rosenthal.ch/downloads/VISCHER-DSE-XS-KMU.pdf

https://dsat.ch

Auskunftsrecht

Eigene Richtlinien erstellen

DSGVO

- Verantwortlicher gibt der betroffenen Person auf Nachfrage:
  - Kopie ihrer Personendaten
  - gewisse Zusatzinformationen
- Betroffene Person kann eine Kopie ihrer Daten verlangen
- Verweigerung offensichtlich unbegründeter/exzessiver Anfragen oder Verlangen einer Gebühr
- Ausnahmen zum Schutz von Dritten und Geschäftsgeheimnissen

Revidiertes DSG

- Gleiches Konzept, aber
  - kürzere Liste der einforderbaren Zusatzinformationen
  - zusätzlich Angaben zu Exporten (Länderliste, Rechtsgrundlagen)
  - Recht, weitere nützliche Informationen zu verlangen
- Mehr Schutz vor Rechtsmissbrauch
- Schwächerer Schutz von Geschäftsgeheimnissen

Busse!

Einschränkungen des Auskunftsrechts

Art. 26 Einschränkungen des Auskunftsrechts

[1] Der Verantwortliche kann die Auskunft verweigern, einschränken oder aufschieben, wenn:

a. ein Gesetz im formellen Sinn dies vorsieht, namentlich um ein Berufsgeheimnis zu schützen;

b. dies aufgrund überwiegender Interessen Dritter erforderlich ist; oder

c. das Auskunftsgesuch offensichtlich unbegründet ist, namentlich wenn es einen datenschutzwidrigen Zweck verfolgt, oder offensichtlich querulatorisch ist.

[2] Darüber hinaus ist es in den folgenden Fällen möglich, die Auskunft zu verweigern, einzuschränken oder aufzuschieben:

a. Der Verantwortliche ist eine private Person und die folgenden Voraussetzungen sind erfüllt:

1. Überwiegende Interessen des Verantwortlichen erfordern die Massnahme.
2. Der Verantwortliche gibt die Personendaten nicht Dritten bekannt.

Nur Abs. 1 und 2 (1. Teil)

Andere Betroffenenrechte

Eigene Richtlinien erstellen

DSGVO

- Recht auf Berichtigung
- Recht auf Löschung/Vergessen
- Recht auf Einschränkung
- Recht auf Widerspruch
- Recht auf Datenübertragbarkeit
- Pflicht, Dritte über die erfolgte Ausübung dieser Rechte zu informieren

Revidiertes DSG

- Vergleichbare Betroffenenrechte
- Schweizer Version des Rechts auf Widerspruch umfasst bereits das Recht auf Löschung/Einschränkung
  - Kann von überwiegenden privaten Interessen verdrängt werden
- Nur wenige Ausnahmen vom Recht auf Berichtigung (Rechtspflicht, Archiv im öffentlichen Interesse)
- Keine Pflicht Dritte zu informieren

Verantwortliche, Auftragsverarbeiter

Verträge anpassen

DSGVO

- DSGVO 28(3) legt den Mindestinhalt von Auftragsdatenverarbeitungs-Verträgen ("ADV") fest
- Beizug von Unterauftragsverarbeiter nur mit Genehmigung des Verantwortlichen
- DSGVO 26 verlangt vertragliche Festlegung der Verantwortlichkeiten von gemeinsamen Verantwortlichen
- Auftragsverarbeiter haften beschränkt

Revidiertes DSG

- Übernahme der Begrifflichkeit Verantwortlicher/Auftragsbearbeiter
- Weniger detaillierte Inhaltsvorgaben für ADV; sollten angepasst werden
  - Verweise auf DSG und Länder-Liste (Datenexporte) hinzufügen, EU SCC mit Schweizer Zusatz
- Keine explizite Vertragspflicht von gemeinsamen Verantwortlichen
- Haftung aller die "mitwirken" an einer Persönlichkeitsverletzung

Busse!

Datenschutzbeauftrager, Vertreter

Keine Anpassungen

DSGVO

- Datenschutzbeauftragter ("DSB") bestellen für Verarbeitungen mit
  - regelmässiger/systematischer Überwachung oder
  - vielen sensitiven Daten
- DSGVO definiert die Unabhängigkeit, den Status, die Aufgaben und andere Voraussetzungen eines DSB
- Ausländische Verantwortliche/ Auftragsverarbeiter müssen unter gewissen Voraussetzungen einen Vertreter in der EU bestellen

Revidiertes DSG

- Keine Pflicht zur Bestellung DSB
- DSG kennt die ähnliche Rolle des "Datenschutzberaters"
  - Voraussetzungen vergleichbar
  - kann DSFAs anstelle der Aufsichtsbehörde beurteilen
- Pflicht zur Bestellung eines lokalen Vertreters, wo Verantwortliche sich auf Personen in der Schweiz ausrichten oder diese beobachten und umfang- und hochrisikoreiche Bearbeitungen haben

Datensicherheit, Privacy by Design

Leichte Anpassungen

DSGVO

- Technische und organisatorische Massnahmen für ein dem Risiko angemessenes Datenschutzniveau
- Massnahmen zur Einhaltung anderer Vorschriften ("Privacy by Design")
- "Privacy by Default"
  - Standardmässige Beschränkung der Verarbeitung auf ein Minimum
  - Keine Veröffentlichung ohne Zustimmung der betroffenen Person

Revidiertes DSG

- Das DSG verlangt dasselbe Datenschutzniveau
- Ähnliche Pflichten bezüglich "Privacy by Design"
- "Privacy by Default"
  - Pflicht, dass Voreinstellungen die am wenigsten invasive Einstellung bezüglich Privatsphäre aufweisen
  - Es kann mit dem Endbenutzer etwas anderes vereinbart werden

Busse!

VISCHER

DSV: Protokollierung, Bearbeitungsreglement

Art. 4 Protokollierung

[1] Werden besonders schützenswerte Personendaten in grossem Umfang automatisiert bearbeitet oder wird ein Profiling mit hohem Risiko durchgeführt und können die präventiven Massnahmen den Datenschutz nicht gewährleisten, so müssen der private Verantwortliche und sein privater Auftragsbearbeiter zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten protokollieren. Eine Protokollierung muss insbesondere dann erfolgen, wenn sonst nachträglich nicht festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie beschafft oder bekanntgegeben wurden.

[2] Das verantwortliche Bundesorgan und sein Auftragsbearbeiter protokollieren bei der automatisierten Bearbeitung von Personendaten zumindest das Speichern, Verändern, Lesen, Bekanntgeben, Löschen und Vernichten der Daten.

[3] Bei Personendaten, welche allgemein öffentlich zugänglich sind, sind zumindest das Speichern, Verändern, Löschen und Vernichten der Daten zu protokollieren.

[4] Die Protokollierung muss Aufschluss geben über die Identität der Person, die die Bearbeitung vorgenommen hat, die Art, das Datum und die Uhrzeit der Bearbeitung sowie gegebenenfalls die Identität der Empfängerin oder des Empfängers der Daten.

[5] Die Protokolle müssen während mindestens einem Jahr getrennt vom System, in welchem die Personendaten bearbeitet werden, aufbewahrt werden. Sie dürfen ausschliesslich den Organen und Personen zugänglich sein, denen die Überprüfung der Anwendung der Datenschutzvorschriften oder die Wahrung oder Wiederherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der Daten obliegt, und dürfen nur für diesen Zweck verwendet werden.

Art. 5 Bearbeitungsreglement von privaten Personen

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

a. besonders schützenswerte Personendaten in grossem Umfang bearbeiten; oder

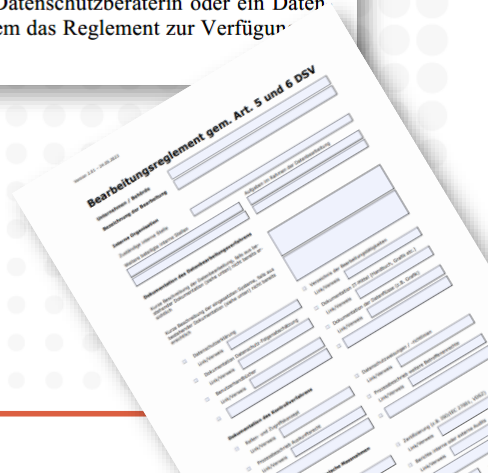
b. ein Profiling mit hohem Risiko durchführen.

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

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

Wird selten sein …

Muster:
https://www.rosenthal.ch/downloads/Bearbeitungsreglement-kurz.pdf



Automatisierte Einzelentscheide

Keine Anpassungen

DSGVO

- Anspruch, keiner automatisierten Entscheidung/Profiling mit negativen rechtlichen oder tatsächlichen Folgen ausgesetzt zu sein
- Solche Entscheidungen sind aber erlaubt für den Abschluss oder die Erfüllung eines Vertrags, sofern per Gesetz erlaubt oder mit Einwilligung
  - Recht auf "menschliches Gehör"
  - Informationspflicht

Revidiertes DSG

- Gleiche Definition automatisierter Einzelentscheide, jedoch ohne die Erwähnung von "Profiling"
- Kein Verbot oder dergleichen
- Ähnliches Recht auf menschliches Gehör und Information, es sei denn die Entscheidung erfolgt
  - so wie von der betroffenen Person gewünscht (z.B. im Online-Shop) oder
  - mit ihrer Einwilligung

Busse!

Data Breach Notifications

Abläufe anpassen

DSGVO

- Verletzung des Schutzes von Personendaten = ungeplanter Bruch der Vertraulichkeit, Integrität oder Verfügbarkeit persönlicher Daten
- Meldung von Verletzungen mit dem Risiko negativer Folgen für die Betroffenen an die Datenschutz-Behörde innerhalb von 72 Stunden
- Meldung an betroffene Person bei Vorliegen hohen Risikos
- Auftragsverarbeiter muss jede Verletzung dem Verantwortlichen mitteilen

Revidiertes DSG

- Verletzung der Datensicherheit gleich definiert wie in der DSGVO
- Auftragsverarbeiter: Wie DSGVO
- Verantwortliche: Meldung an Behörde nur bei hohem Risiko
- Keine 72-Stunden-Frist, keine Pflicht zur Protokollierung der Verletzungen
- Meldung an betroffene Person, falls es "zu ihrem Schutz erforderlich" ist
- Ausnahme bei übermässigem Aufwand

Regeln für Datenexporte

Andere, aber ähnliche Abläufe

DSGVO

- Keine Übermittlung in Länder ohne angemessenes Datenschutzniveau (ausser Vorliegen einer Ausnahme oder einer Schutzmassnahme)
- EK entscheidet über Angemessenheit
- Übliche Schutzmassnahmen: Standard-Vertragsklauseln ("SCC"), Binding Corporate Rules ("BCR")
- Ausnahmen u.A. bei Einwilligung oder für Vertragserfüllung oder im Rahmen von Behörden- und Gerichtsverfahren

* https://www.rosenthal.ch/downloads/VISCHER-faq-scc.pdf

Revidiertes DSG

- Dasselbe Konzept
- Knüpft an Übermittlung über die Schweizer Grenzen hinaus an
- Angemessenheit bestimmt durch Bundesrat (folgt im Prinzip der EU, Ausnahme für Japan, Südkorea)
- Verwendung von EU SCC (mit EDÖB-Zusatz*) und BCR im Rahmen des DSG grundsätzlich möglich
- Ähnliche Ausnahmen

Busse!

Dokumentationspflichten

Kleine Anpassungen

DSGVO

- Verzeichnis der Verarbeitungs-tätigkeiten
  - für Verantwortliche/Auftragsver.
  - definierter Inhalt
- Rechenschaftspflicht (DSGVO 5(2))
- Datenschutz-Folgenabschätzung
  - für Verarbeitungen mit vermutungsweise hohem Risiko
  - Pflicht, die Aufsichtsbehörde zu konsultieren bei hohem Risiko trotz getroffener Massnahmen

Revidiertes DSG

- Selbes Verzeichnis verwenden
  - Exportländer aus Schweizer Sicht
  - KMU-Ausnahme greift weiter
- Vergleichbare Pflicht zur Vornahme Datenschutz-Folgenabschätzung
  - Rechtsgrundlage muss darin nicht genannt werden
  - Konsultation EDÖB *oder* DSB
  - DSFA 2 Jahre länger aufbewahren
- Keine Rechenschaftspflicht

Bearbeitungsverzeichnis, DSFA

Art. 24 Ausnahme von der Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten

Unternehmen und andere privatrechtliche Organisationen, die am 1. Januar eines Jahres weniger als 250 Mitarbeiterinnen und Mitarbeiter beschäftigen, sowie natürliche Personen sind von der Pflicht befreit, ein Verzeichnis der Bearbeitungstätigkeiten zu führen, ausser eine der folgenden Voraussetzungen ist erfüllt:

a. Es werden besonders schützenswerte Personendaten in grossem Umfang bearbeitet.

b. Es wird ein Profiling mit hohem Risiko durchgeführt.

Art. 24 DSV

Art. 69 revDSG

Art. 69 Übergangsbestimmungen betreffend laufende Bearbeitungen

Die Artikel 7, 22 und 23 sind nicht anwendbar auf Datenbearbeitungen, die vor Inkrafttreten dieses Gesetzes begonnen wurden, wenn der Bearbeitungszweck unverändert bleibt und keine neuen Daten beschafft werden.

Berufsgeheimnis

persönliche Strafbarkeit

DSGVO

- Gibt es in der DSGVO so nicht

Art. 62 Verletzung der beruflichen Schweigepflicht

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

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

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

Revidiertes DSG

- Schweigepflicht für alle Berufsleute
  - für in Ausübung des Berufes erfahrene geheime Personendaten
  - sofern deren Kenntnis für die Ausübung des Berufes nötig ist
- Nur vorsätzliches Handeln erfasst
- Schutz der Kunden; Verzicht ist möglich, aber nicht immer nötig
- Persönliche Busse bis CHF 250'000

Busse!

Durchsetzung und Bussen

persönliche Strafbarkeit

DSGVO

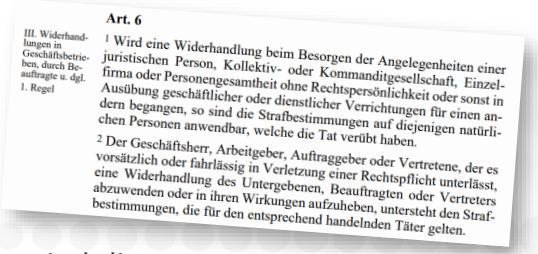
- Datenschutz-Aufsichtsbehörden können
  - Verarbeitungsvorgänge untersuchen
  - Verfügungen zur Einstellung, Einschränkung oder Anpassung einer Verarbeitung erlassen
  - Für die meisten Verstösse: Bussen bis EUR 10/20 Mio. oder 2/4% des weltweit erzielten Jahresumsatzes
- Ev. weitere Bussen gemäss lokalem Recht

Revidiertes DSG

- Die Datenschutz-Aufsichtsbehörde (EDÖB) kann
  - Bearbeitungsvorgänge untersuchen
  - Verfügungen zur Einstellung, Einschränkung oder Anpassung der Verarbeitung erlassen
- Kantonale Strafbehörden können
  - Persönliche Bussen bis CHF 250’000 verfügen für Verletzung gewisser DSG-Bestimmungen und mangelnde Kooperation mit dem EDÖB
  - Bussen sind nicht versicherbar

Busse!

Strafbarkeit



III. Widerhandlungen in Geschäftsbetrieben, durch Beauftragte u. dgl.
1. Regel

Art. 6

[1] Wird eine Widerhandlung beim Besorgen der Angelegenheiten einer juristischen Person, Kollektiv- oder Kommanditgesellschaft, Einzelfirma oder Personengesamtheit ohne Rechtspersönlichkeit oder sonst in Ausübung geschäftlicher oder dienstlicher Verrichtungen für einen andern begangen, so sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar, welche die Tat verübt haben.

[2] Der Geschäftsherr, Arbeitgeber, Auftraggeber oder Vertretene, der es vorsätzlich oder fahrlässig in Verletzung einer Rechtspflicht unterlässt, eine Widerhandlung des Untergebenen, Beauftragten oder Vertreters abzuwenden oder in ihren Wirkungen aufzuheben, untersteht den Strafbestimmungen, die für den entsprechend handelnden Täter gelten.

VStrR

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

"Bei Widerhandlungen in Geschäftsbetrieben … sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar …"

Strafrechtliche Verantwortlichkeit

- Auskunftsrecht
- Informationspflicht
- Pflicht zum AVV
- Bekanntgabe ins Ausland
- Datensicherheit
- Weisungen des EDÖB
- Berufsgeheimnis (tw.)

Durch Handeln

Jeder, der handelt

Beispiele:

- Wer in Kauf nimmt, eine falsche Auskunft an einen Betroffenen zu erteilen
- Wer entscheidet, die Datenschutz-Erklärung nicht wie erforderlich nachzuführen

Durch Unterlassen

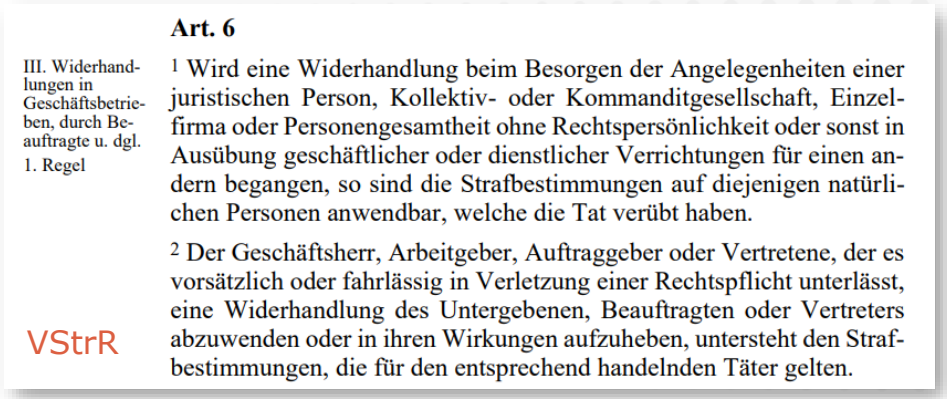
Wer eine Garantenstellung hat

- Wer als GL-Mitglied nicht dafür sorgt, dass Auskunftsersuchen richtig behandelt werden
- Wer als leitender Inhaber einer Bearbeitung keine korrekte DSE in Auftrag gibt
- Der untätige VR, weil er keinen Bericht will

1. Person muss Pflicht haben, Rechtsverletzungen zu verhindern und die dafür nötigen Befugnisse
2. Sie kommt ihrer Pflicht zur sorgfältigen Auswahl, Instruktion und Überwachung nicht nach

Datenschutzstelle: Weisungs-/Interventionsrecht?

- Ermöglicht **Durchsetzung** der Datenschutz-Compliance
- Aber:
  - Führt zu unnötigen internen **Konflikten**
  - Führt zu strafrechtlicher **Verantwortlichkeit**



III. Widerhandlungen in Geschäftsbetrieben, durch Beauftragte u. dgl.
1. Regel

Art. 6

1 Wird eine Widerhandlung beim Besorgen der Angelegenheiten einer juristischen Person, Kollektiv- oder Kommanditgesellschaft, Einzelfirma oder Personengesamtheit ohne Rechtspersönlichkeit oder sonst in Ausübung geschäftlicher oder dienstlicher Verrichtungen für einen andern begangen, so sind die Strafbestimmungen auf diejenigen natürlichen Personen anwendbar, welche die Tat verübt haben.

2 Der Geschäftsherr, Arbeitgeber, Auftraggeber oder Vertretene, der es vorsätzlich oder fahrlässig in Verletzung einer Rechtspflicht unterlässt, eine Widerhandlung des Untergebenen, Beauftragten oder Vertreters abzuwenden oder in ihren Wirkungen aufzuheben, untersteht den Strafbestimmungen, die für den entsprechend handelnden Täter gelten.

VStrR

Pflicht zur Überwachung
+
Entscheidungsgewalt
=
Garantenstellung

Sicherer: Reines Berichtsrecht an GL/VR

Rollenverteilung

https://www.vischer.com/know-how/blog/wie-strafbarkeit-unter-dem-neuen-datenschutzgesetz-vermieden-wird/

- **Verwaltungsrat** (D: "Aufsichtsrat)
  - Oberaufsicht über die Einhaltung des Datenschutzes
  - Delegiert die Umsetzung an die GL
- **Geschäftsleitung** (D: "Vorstand")
  - Trifft die nötigen Massnahmen zur Umsetzung im Betrieb
  - Trifft die nötigen Entscheide zur Bearbeitung
- **Datenschutzstelle** ("Data Protection Compliance Officer")
  - Erarbeitung der Vorgaben, Beratung in deren Umsetzung, Überprüfung deren Umsetzung, Inhaber Datenschutzprozesse
- **Inhaber der Datenbearbeitungen** ("Data Activity Owner")
  - Treffen die nötigen Entscheide und sorgen für deren Umsetzung

In Grundsätzen regeln

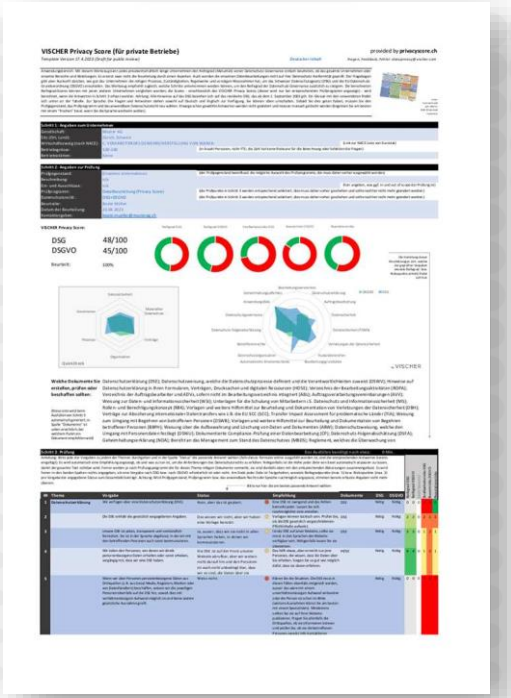
In Datenschutz-weisung regeln

Pflichten der GL bzw. des VR

- Angemessene …
  - **Auswahl**
  - **Instruktion** (inkl. Bereitstellung von Ressourcen)
  - **Überwachung**

- Es genügt nicht, die GL mit der Umsetzung des Datenschutzgesetzes zu beauftragen
  - VR muss sich **berichten lassen** (GL auch)
  - **Durch Datenschutzstelle**, direkt oder indirekt via Compliance

Beispiel:
https://privacyscore.ch (oder Excel)



revDSG – was zu tun ist.

Für KMU · Umgesetzt: ☑ · Neu ab 1.9.2023

7 Zehn Gebote zum Umgang mit Personendaten nach DSG[1]

1. Wir **sagen** der Person vorher, was wir mit ihren Daten wozu tun.
2. Wir **halten uns daran** und setzen Daten nicht zweckwidrig ein.
3. Wir üben uns in **Datensparsamkeit** und "need-to-know".
4. Wir **löschen rasch**, was wir nicht mehr brauchen.
5. Wir erlauben einer Person auch **"Nein"** zu sagen.
6. Wir tun nur das, was wir bei uns selbst **akzeptabel** fänden.
7. Wir prüfen unsere Daten auf problematische **Fehler** und Lücken.
8. Wir geben **sensitive Daten**[2] nicht für Zwecke Dritter weiter.
9. Wir treffen Massnahmen, damit die Daten bei uns **sicher** sind.
10. Wir beschaffen Daten auf **legale Weise** und aus legalen Quellen.

Ausnahmen sind (nur) bei "besserem" Grund möglich.
Wir gestalten jede Datenbearbeitung nach diesen Geboten!

2 Datenschutzerklärung

Jede planmässige, gesetzlich nicht erforderliche Beschaffung von Personendaten ist in der Datenschutzerklärung ("DSE"). Wir weisen die Personen auf die DSE hin (AGB, Formulare, Apps etc.). Sie ist auf unserer Website.
Pflichtinhalt: Wer wir sind (mit Kontaktangaben), wozu wir die Daten beschaffen, welche Daten, wem wir sie geben (Namen nicht nötig), in welche Länder oder Regionen sie gehen können und worauf wir uns rechtlich stützen.[3]

1 Inventar der Bearbeitungen

Wir führen ein Verzeichnis unserer Aktivitäten, bei denen Personendaten bearbeitet werden (z.B. Verwaltung der Kundendaten, Buchhaltung, Personalverwaltung, Onlineshop). Aufgeführt ist der Inhalt gemäss Art. 12 revDSG, u.a. Bearbeitungszwecke, Kategorien von Personen, Daten und Empfänger, Aufbewahrungsdauer.[4] Diese **Pflicht gilt nur**, falls wir 250+ Mitarbeiter (Köpfe) haben oder sensitive Daten[2] in grossem Umfang bearbeiten oder Hochrisiko-Profiling betreiben.

3 Auftragsbearbeiter

Falls wir einem IT-Provider oder sonst jemandem die Bearbeitung unserer Daten anvertrauen, schliessen wir einen "ADV" ab, d.h. einen **Vertrag**, der uns erlaubt ihn zu steuern und zu kontrollieren und den Beizug von Dritten vorab zu genehmigen (oder ihm zu widersprechen). Er hält auch die **Sicherheitsmassnahmen** (sog. TOMS) fest. Diese prüfen wir (ggf. inkl. Audit-Berichte). Ein ADV nach Art. 28 DSGVO genügt, falls er ebenso auf das DSG verweist. Der Auftragsbearbeiter darf nur tun, was wir auch tun dürfen (z.B. i.d.R. keine Datennutzung für sich). Wir prüfen die heutigen/neuen ADV auf Konformität.

5 Wenn Daten ins Ausland gehen

Problemlos: EWR, UK, angemessene Länder[5]

Alle **anderen Staaten** u.a. erlaubt falls:

- Export zur Abwicklung eines Vertrages mit oder für die betroffene Person nötig
- Expliziter Verzicht auf Schutz im Ausland
- Abschluss der "Standardvertragsklauseln" der EU[6] mit CH-Anpassung und keinen Grund zur Annahme haben, dass es zu problematischen Behördenzugriffen kommt (→ TIA machen[6,7])

Wir prüfen unsere Verträge daraufhin!

4 Die Daten sind sicher, sonst melden wir

Technisch: Zugang nur "need-to-know" und mit persönlichem Konto, "MFA" bei externem Zugriff, Audit-Trails (ggf. Pflicht bei sensitiven Daten[2], 1 Jahr), Pseudonymisierung, Firewalls, Antimalware-Software, Backups (auch offline).
Organisatorisch: Weisungen (z.B. dieses Blatt dazu verwenden), Schulungen, Prüfung der Logs, Prüfung der Massnahmen, bei vielen sensitiven Daten[2] Bearbeitungsreglement.
Meldepflicht: Ist die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten verletzt *und* das Risiko negativer Folgen für einzelne Personen hoch (nicht bloss lästig) → EDÖB melden (Formular auf https://edoeb.admin.ch) und für 2 Jahre dokumentieren; können sich Personen selbst vor Folgen schützen → Meldung auch an sie.

Jeder ist für Sicherheit mitverantwortlich!

6 Wir gewähren Betroffenen ihre Rechte

Wir **identifizieren** die Person vorgängig richtig.
Wir geben einer Person **Auskunft** über ihre eigenen Personendaten (nicht Dokumente) und auf Wunsch bestimmte weitere Infos (i.d.R. gratis innert 30 Tagen). Wir vermeiden den Eindruck, es seien alle Daten gegeben (falsche oder unvollständige Auskunft ist strafbar). Wir können zuerst nur gängige Daten liefern. Die Person muss beim Finden mitwirken. Datenschutzfremde Zwecke sind nicht geschützt. Wir schützen Daten Dritter und eigene Geschäftsgeheimnisse.
Jede Person kann **Datenkorrektur** verlangen. Ist die Wahrheit umstritten, vermerken wird dies.
Jede Person kann **Löschung** ihrer Daten verlangen oder sonst wollen, dass wir unsere Bearbeitung stoppen oder ändern. Wir können weitermachen, falls wir einen besseren Grund dafür haben.
Trifft bei uns ein **Computer** Ermessensentscheide mit wichtigen negativen Folgen, sagen wir das den Betroffenen und bieten menschliches Gehör an.
In bestimmten Fällen müssen wir Personendaten, die wir erhalten und als Historie haben, den Personen zwecks Weiterverwendung **herausgeben**.

Wir stellen sicher, dass wir das können!

7 Wir verlassen uns nicht auf Einwilligungen

Wir stützen uns grundsätzlich nicht auf Einwilligungen. Falls doch, müssen sie **informiert** und **freiwillig** erfolgen, bei sensitiven Daten[2] und Hochrisiko-Profiling explizit.

10 Datenschutz Folgenabschätzung (DSFA)

Bei Vorhaben, die punkto Datenbearbeitung für Betroffene **risikoreicher** sein könnten, machen wir eine DSFA. Darin dokumentieren wir das Vorhaben und die Massnahmen zu ihrem Schutz und prüfen, ob trotzdem hohe Risiken unerwünschter **negativer Folgen** für sie bleiben (falls ja: Hilfe holen). Wir bewahren sie auf.

8 Privacy by Default

Wo wir in Apps, auf Websites etc. **Einstellungen** zum Datenschutz haben, sind diese auf das **Minimum** voreingestellt. Die Entwickler achten darauf.

9 Kleines Berufsgeheimnis

Zeigt an, dass vorsätzliche Verletzung strafbar ist (bis CHF 250k, auf Antrag)

Uns **anvertraute**, beruflich nötige Personendaten halten wir geheim oder wir stellen vorab klar, dass wir die Daten nicht geheim halten werden.

Wir haben eine Stelle, die weiss was zu tun ist, wenn … (5 7 10 4)

… eine Person ihre Daten sehen/haben oder diese gelöscht oder korrigiert haben will oder sie sonst ein sie betreffendes Datenschutzanliegen hat:

… wir ein neues oder geändertes Vorhaben haben, das auch Daten von Personen betrifft und daher der Datenschutz (ggf. mit DSFA) geprüft werden muss:

… Daten von Personen verloren gehen, in falsche Hände gelangen, manipuliert wurden, dies passiert sein könnte oder es Sicherheitsprobleme gibt:

Jeder von uns meldet solche Vorkommnisse dieser Stelle umgehend!

[1] revDSG/DSV: https://datenrecht.ch/gesetzestexte
[2] Besonders schützenswerte Daten: Art. 5 Bst. c revDSG
[3] Vgl. Musterdatenschutzerklärung auf https://dsat.ch
[4] Vorlagen: https://dsat.ch, https://bit.ly/3qrpOIb
[5] Vgl. Anhang I der DSV (https://bit.ly/3DmSbPm)
[6] Vgl. FAQ (mit Bezugsquellen): https://bit.ly/3qvGJZ5
[7] Vgl. TIA: https://bit.ly/3L3mxYO (mit Verweis auf FAQ)

Fragen? (FAQ auf https://bit.ly/3RC49c1 und mehr auf https://bit.ly/3RCmuRQ)
Intern:
Extern:

Legende: Umgang mit Daten · Governance · Prio Umsetzung · Umgesetzt ja/nein

Version 13.9.2022 – Updates: www.rosenthal.ch – Hier ist das revDSG strenger als die DSGVO oder erfordert andere, inkompatible Abläufe. Strafbar

Autor: David Rosenthal, drosenthal@vischer.com Alle Rechte vorbehalten. Darf (ausser in den Feldern) unverändert frei weitergegeben/benutzt werden. Dies ist Information, keine Rechtsberatung. CC BY ND „VISCHER

Alles auf einer einer Seite.

https://www.rosenthal.ch/downloads/VISCHER-revDSG-Survival-Guide.pdf

Schlussbemerkungen

- Wer für die DSGVO fit ist, wird in der Schweiz **keinen grossen Aufwand** haben
- Die Vorgaben sind vergleichbar mit jenen der DSGVO, doch hat die Schweiz **einen pragmatischeren Ansatz** gewählt, was sich im Tagesgeschäft auszahlt
- Allerdings sollten **Weisungen**, die **Datenschutzerklärung** und **Auftragsbearbeitungsverträge** angepasst werden
- Differenzen zwischen der DSGVO und dem DSG werden oft erst im Umgang mit **Einzelfällen** (z.B. bei Streitigkeiten über das Auskunftsrecht) von Relevanz sein – dies ist vorzusehen
- Keiner kann das DSG vollständig einhalten – das bleibt so

VISCHER

Vielen Dank für die Aufmerksamkeit!

Fragen: drosenthal@vischer.com

Weiteres Material:
www.rosenthal.ch

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com