VISCHER

Revision Datenschutzgesetz:

Zehn Schritte zur Umsetzung der neuen gesetzlichen Anforderungen für Unternehmen

David Rosenthal
13. Oktober 2020

Was erwartet Sie?

Ausführliche kostenlose Kommentierung erscheint im November

- Am 25. September 2020 verabschiedete das Parlament eine **Totalrevision des Datenschutzgesetzes** (DSG)
  - Text: https://bit.ly/34PmN9h (Vergleich: datenrecht.ch)
  - Jetzt folgen die Verordnungen, mit einer Vernehmlassung (Q1)
  - Inkrafttreten erst in 2022, aber *ohne* Übergangsfrist
- Die Schweiz **schliesst im Datenschutz zur EU auf**
- Aber: Materiell **keine fundamentale Veränderung**
  - Bisher erlaubte Bearbeitungen sind i.d.R. weiterhin erlaubt
  - Keine Kopie der EU-Datenschutz-Grundverordnung (DSGVO), aber viele Regelungen werden übernommen → sep. Webinar
  - Ausgebaut werden die Governance und Betroffenenrechte

Schritt 1: Datenschutzerklärung

Für die DSGVO formulierte Datenschutzerklärungen gehen weiter, können aber mit den passenden Anpassungen auch für das DSG verwendet werden

- Ab dem neuen DSG wird sie zur Pflicht
  - Informiert werden muss bei jeder Daten*beschaffung*
  - Aufschalten auf eigener Website, AGB/Formulare mit Link
- Gesetz definiert Mindestinhalt, mehr nur ausnahmsweise nötig
  - Identität, Zweck jeder Beschaffung, Kategorien der Empfänger, Kategorien der Daten (falls nicht bei der Person selbst beschafft), Länder und Rechtfertigung des Exports in unsichere Drittstaaten
- Vorsätzliche Verletzung kann gebüsst werden (CHF 250'000)
- **Praxistipp:** Erheben Sie frühzeitig im Betrieb, wer welche Daten wozu beschafft, damit die Formulierung leichter fällt
  - Nicht abgedeckt werden müssen gesetzliche Datenbearbeitungen

Schritt 2: Verzeichnis erstellen

Für die DSGVO erstellte Verzeichnisse können Sie direkt übernehmen

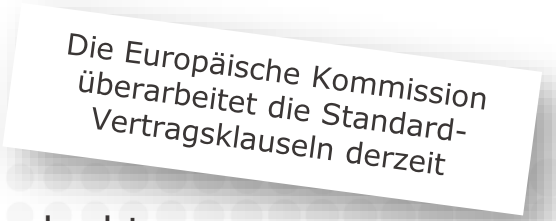
- Alle Datenbearbeitungen müssen verzeichnet werden
  - Wie Sie das Verzeichnis strukturieren, ist Ihnen überlassen
  - Muss nicht detailliert sein, enthält nicht die Personendaten
  - Excel/Word statt teurer Programme genügen oft (→ dsat.ch)
- Gesetz definiert Mindestinhalt
  - Identität, Zweck der Bearbeitung, Kategorien der Empfänger, Kategorien der Daten, Aufbewahrungsdauer, Länder und wie Exporte in unsichere Drittstaaten abgesichert werden
  - Kürzere Liste für Auftragsbearbeiter
- **Praxistipp:** Kombinieren Sie dies mit Schritt 1 und lassen Sie die "Linie" ihre Teile im Verzeichnis regelmässig nachführen
  - Aber: Verletzung der Vorschrift wird nicht sanktioniert

Schritt 3: Auftragsbearbeitungen

Für die DSGVO erstellte Verträge können Sie mit Anpassungen übernehmen

- Wer einem Dienstleister die Bearbeitung von Personendaten überträgt, muss mit diesem einen Vertrag abschliessen
  - Weisungsrecht, Kontrollrecht, Unterstützung bei DSG-Compliance
  - Sicherstellen der Datensicherheit
  - Beizug von Unterauftragsbearbeitern nur mit Genehmigung (neu)
- Aber: Bearbeitet er die Daten für sich selbst oder bestimmt er die wesentlichen Aspekte, so ist dieser selbst "Verantwortlicher"
  - Trotzdem sollte mit ihm ein Vertrag abgeschlossen werden
- Vorsätzliche Verletzung kann gebüsst werden (CHF 250'000)
- **Praxistipp:** Mit den meisten Dienstleistern werden Sie bereits passende Verträge haben; sichten Sie sie aber zur Sicherheit

Schritt 4: Auslandstransfers



- Datentransfers in "unsichere" Drittstaaten sind nur mit besonderen Vorkehrungen oder in Ausnahmefällen erlaubt
  - Neu legt der Bundesrat fest, welche Länder als "unsicher" gelten
  - Schweizer Regelung entspricht weitgehend der DSGVO
- Bei unsicheren Drittstaaten werden in der Regel die Standard-Vertragsklauseln der Europäischen Kommission verwendet
  - Wegen "Schrems II" gelten diese für die USA tw. als ungenügend
- Wichtigste Ausnahme: Vertragsabwicklung, Rechtsverfahren
- Vorsätzliche Verletzung kann gebüsst werden (CHF 250'000)
- **Praxistipp:** Wissen Sie, wo überall Daten in unsichere Staaten fliessen? Regeln Sie Datenflüsse vertraglich, auch im Konzern

Schritt 5: DSFA

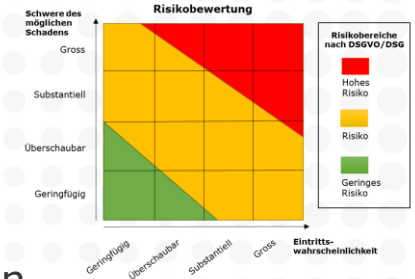
Für die DSGVO erstellte DSFAs können Sie unter dem DSG weitgehend übernehmen

- Bei tendenziell heiklen Datenbearbeitungen muss neu vorgängig eine "Datenschutz-Folgenabschätzung" (DSFA) durchgeführt werden
  - Selbstbeurteilung eines Vorhabens durch den Verantwortlichen
  - Inhalt: Beschreibung, Analyse der möglichen (unbeabsichtigten) negativen Folgen für eine betroffene Person, Gegenmassnahmen
- Birgt ein Vorhaben trotz aller Massnahmen ein hohes Risiko, muss der EDÖB (oder Datenschutzberater) konsultiert werden
  - Aber: Verletzung wird nicht sanktioniert
- **Praxistipp:** Erstellen Sie die DSFA zusammen mit der Linie, denn nur diese kennt das jeweilige Vorhaben hinreichend gut und weiss, welche Massnahmen noch getroffen werden könnten

Schritt 6: Data Breach Notifications

Unter dem DSG werden weniger Meldungen erfolgen müssen als unter der DSGVO

- Verletzung der Datensicherheit: Unplanmässiger Bruch der Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten
  - Beispiele: Falsch versendete Mail, Datenverluste, Hacker-Zugriffe
- Meldung an EDÖB nur, falls ein «hohes Risiko» negativer Folgen für Betroffene besteht (konkrete, nicht theoretische Gefahr)
  - Meldung sobald die vorgeschriebenen Angaben vorliegen
  - Aber: Verletzung wird nicht sanktioniert
- Muss der betroffenen Person mitgeteilt werden, falls dies zu ihrem Schutz nötig ist (z.B. um Passwort zu ändern)
- **Praxistipp:** Bestimmen Sie eine zuständige Stelle und weisen sie die Mitarbeiter an, ihr entsprechende Vorfälle zu melden
  - Auftragsbearbeiter müssen ebenfalls alle Verletzungen melden



VISCHER

Einbruch in Arztpraxis, wohl zur Beschaffung von Drogen, nicht den Patientenakten

Versicherungsagentur entsorgt Akten ständig ungeshreddert im offenen Abfall, Nachbar meldet es

Online-Shop gehackt, Passwörter gestohlen, nur einfach gehasht

Nicht besonders heikle E-Mail versehentlich an falschen, aber vertrauenswürdigen Empfänger

Mitarbeiter einer Bank entwendet Kundendaten

Firewall-Hersteller entdeckt alte Sicherheitslücke, die fremden Zugriff erlaubt, liefert Patch; kein Hinweis auf Zero-Day-Exploit

Professor verliert Prüfungsbögen, Prüfung muss wiederholt werden

Mitarbeiter unterhalten sich über heikle und vertrauliche Personalie im Zug für Dritte mithörbar, jedoch keine nützlichen Hinweise auf die Identität für Aussenstehende

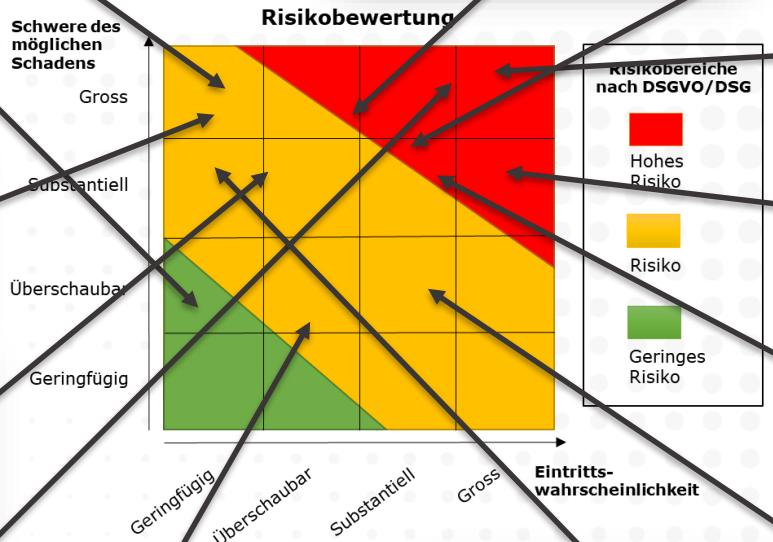
Bank versendet aufgrund eines Fehlers hunderte Kontoauszüge natürlicher Personen an die falschen Kunden

Ausländische Strafbehörde beschlagnahmt Daten bei einem Cloud-Provider wider Schweizer Recht

Golf-Shop versendet Werbemail versehentlich mit offenen Empfängern

Mitarbeiter verliert USB-Stick mit unverschlüsselten Lohndaten, Stick taucht aber rasch wieder auf

Online-Shop fällt temporär aus, kein Zugriff auf frühere Bestellungen



Schritt 7: Betroffenenrechte

Auskunftsersuchen können oft standardisiert beantwortet werden; bereiten Sie dies vor

- Betroffene Personen können Auskunft über ihre Daten (teils sogar Herausgabe in elektronischer Form) und Korrekturen verlangen sowie einer Datenbearbeitung widersprechen
  - Betroffenenrechte sind i.d.R. kostenlos, gelten nie absolut
  - Identifikation der betroffenen Person wichtig
  - Bedeutung des Rechts auf "Datenportabilität" noch unklar
- Neu mehr Schutz vor missbräuchlichen Auskunftsersuchen
  - Reaktion innert 30 Tagen nötig, Vollständigkeitserklärung nicht
  - Vorsätzliche Verletzung kann gebüsst werden (CHF 250'000)
- **Praxistipp:** Bestimmen Sie eine zuständige Stelle für solche Anfragen und zapfen Sie rechtzeitig die nötigen Datenquellen an

Schritt 8: Maschinelle Entscheide

Die DSGVO kennt eine ähnliche, aber etwas strengere Regel

- Automatisierte Einzelentscheide = Ermessensentscheid mit rechtlichen oder gewichtigen anderen negativen Folgen, den alleine ein Computer bezüglich einer einzelnen Person trifft
  - Beispiel: Automatische Bewerber-Selektion oder Kreditvergabe
  - Nicht erfasst sind reine "Wenn-Dann"-Fälle oder Entscheide, die ein Computer lediglich vorbereitet hat
  - Grundsätzlich zulässig, betroffene Person muss jedoch informiert und auf Wunsch von einem Menschen angehört werden
- Der Schutz besteht nicht, wo die Person in die Automatisierung des Entscheids eingewilligt hat oder es um einen Vertrag geht und so wie verlangt entschieden wird (z.B. Online-Shop-Kauf)
- **Praxistipp:** Automatisierte Einzelentscheide kommen nicht oft vor, führen Sie aber rechtzeitig eine Erhebung im Betrieb durch

Schritt 9: Weitere Neuerungen

Häufigstes Problem ist, dass Daten länger als erforderlich aufbewahrt werden

- Genetische und biometrische Daten gelten neu als besonders schützenswerte Personendaten
  - Folge: Weitergabe an Dritte erfordert eine Rechtfertigung, Einwilligungen müssen neu ausdrücklich erfolgen
- Datenbearbeitungen für nicht-personenbezogene Zwecke (z.B. viele Sekundärnutzungen) unterliegen leicht strengeren Regeln
- Pflicht zum "Privacy by Default": Standard-Voreinstellungen zum Datenschutz in Online-Diensten auf das Minimum setzen
- Profiling mit und ohne "hohem Risiko" wurde zwar eingehend diskutiert, aber nicht mehr eingeschränkt als schon bisher war
- **Praxistipp:** Nehmen Sie die Revision zum Anlass, Ihre Datenbearbeitungen risikobasiert auf ihre Konformität zu prüfen

Schritt 9: Weitere Neuerungen

Prüfen Sie, ob eine Erweiterung Ihrer AGB und Datenschutzerklärungen sinnvoll ist

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.

Schritt 10: Weisungen, Schulung

Sie sollten Datenschutz-Knowhow nach Möglichkeit auch intern aufbauen

- Ohne passende Weisungen und Arbeitsanleitungen wissen Ihre Mitarbeiter nicht, was sie tun müssen und dürfen
  - Passen Sie die Weisungen und Anleitungen rechtzeitig an
  - Erstellen Sie Muster und Vorlagen
  - Führen Sie Schulungen durch, mit Protokollierung der Teilnahme
  - Damit dokumentieren Sie die Einhaltung des DSG, sollten Sie einst Ziel eines Verfahrens werden
- Aber: Interner Datenschutzbeauftragter weiterhin keine Pflicht
- **Praxistipp:** Die Neuerung, dass gewisse Datenschutzverstösse zur persönlichen Strafbarkeit führen können, wird motivieren
  - Strafverfolgung ist Sache der Kantone, nicht des EDÖB

Schlussbemerkungen

Tizian, 1548

- Datenschutz-Compliance ist eine **Sisyphus-Arbeit**
  - Niemand hält das DSG vollständig ein
- **Beginnen Sie** bereits jetzt mit den Umsetzungsarbeiten
  - Hohe Abhängigkeit von anderen Stellen im Betrieb
  - Diese haben nebst ihrem Tagesgeschäft nur wenig Zeit und Lust für Arbeiten zur Datenschutz-Governance
  - Manche der neuen Anforderungen werden schon heute erwartet, sei es vom EDÖB, der DSGVO oder im Rahmen einer guten Datenschutz-Compliance und Governance
- Die Grundprinzipien der Datenbearbeitungen ändern sich nicht, aber werden mehr in den Fokus der **Aufmerksamkeit** gerückt
  - Mehr Verfahren sind zu erwarten, viele Bussen wohl nicht

VISCHER

Melden Sie sich für Updates unseres **Data & Privacy Blogs** an auf www.vischer.com

Danke für Ihre Aufmerksamkeit!

Bei Fragen: drosenthal@vischer.com

Falls Sie eine kostenlose Kopie meiner ausführlichen Kommentierung der Neuerungen möchten, senden Sie mir eine Mail (erscheint im November).

Übersicht: https://bit.ly/2SYo2xv

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