VISCHER

Das revidierte Datenschutzgesetz.
Neuerungen für das Online-Marketing

David Rosenthal, Rolf Auf der Maur, Partner, VISCHER AG
24. April 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
  - **Aber:** Persönliche **Strafbarkeit** bei bestimmten Verletzungen
- Dazu eine gemeinsamen **Branchenempfehlung** von IAB, VSM, LSA und SWA für den Datenschutz für das Online-Marketing

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!

Was wichtig ist

- Verstehen Sie, welche **Rolle** Sie haben:
  - **Controller** / Verantwortlicher – derjenige, der die Ausgestaltung einer Datenbearbeitung definiert
    - z.B. Publisher, Betreiber eines Ad-Netzwerks
    - Gemeinsame Controller = "Joint Controller"
  - **Processor** / Auftragsbearbeiter – wer Personendaten für einen Verantwortlichen bearbeitet
    - z.B. Analytics-Betreiber, Webhoster
- **Darum ist das wichtig:**
  - Viele der DSG-Pflichten knüpfen daran an (z.B. Pflicht zur Datenschutzerklärung)

Was wichtig ist

- Führen Sie Ihre **Datenschutzerklärung** (DSE) nach
  - Neue Vorgaben, die über die DSGVO hinaus gehen
  - Sie sollte nicht nur die Website bzw. die Apps abdecken
  - Eine separate DSE für die eigenen Mitarbeiter
  - Meist wird kein Versand der neuen DSE nötig sein
  - Aber: Wer fremde Verantwortliche auf seiner Website einbindet, sollte auch auf deren DSE hinweisen
- **Darum ist das wichtig:**
  - Jeder sieht die DSE
  - Fehlende / unvollständige DSE kann strafbar sein


Datenschutzerklärung.

Worum geht es?

Wir beschaffen in unserem Geschäft diverse Personendaten[1]. Hier informieren wir Sie wie im Datenschutzgesetz vorgeschrieben.

Wer sind wir?

Das sind wir und unsere Kontaktdaten:

Welche Personendaten beschaffen wir?

Neben den Angaben, die Sie selbst uns mitteilen (durch das, was Sie uns sagen und was Sie bei uns tun[2]), kann es sein, dass wir auch bei Drittquellen Angaben über Sie beschaffen, nämlich:

- Sie betreffende Angaben eines **Kunden** oder Ihres **Arbeitgebers**, mit dem wir zu tun haben (z.B. Ihre Kontaktangaben)
- **Bonitätsauskünfte**
- Sie betreffende **Aufträge**, die wir von Dritten erhalten (z.B. wenn wir Ihnen etwas liefern oder für Sie tun sollen)
- **Belege**, die Sie betreffen, Vollmachten
- Auszüge staatlicher **Register** (z.B. HR)
- Angaben aus **rechtlichen Verfahren**, in denen Sie vorkommen; Zeugenaussagen
- **Empfehlungen**/Hinweise Dritter auf Sie
- Ihre **Social-Media/Online**-Aktivitäten
- **Publikationen**, in denen Sie vorkommen

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.

Wozu beschaffen wir Personendaten?

Wir tun das für folgende Zwecke (nebst denen, die wir Ihnen separat mitteilen):

- **Kommunikation** mit Ihnen
- **Vertragsabschluss/-abwicklung** mit Ihnen (ggf. inkl. zwecks Beschäftigung), Ihrem Arbeitgeber und Kunden
- Betrieb der **Infrastruktur**, Website, App
- **Marketing** (z.B. Mailings, mit Abmelde-Link/Option, Anlässe), Beziehungspflege
- **Marktanalysen**, Planung, Entwicklung von Produkten & Dienstleistungen, F&E
- **Compliance** (Einhaltung von Gesetzen, Branchenstandards, Weisungen etc.)
- **Rechtliche Verfahren**, Untersuchungen
- Wahrung **Sicherheit**, Zugangskontrolle
- **Geschäftsführung**, Risiko-Management
- Unternehmenstransaktionen (z.B. **M&A**)
- **PR**, Aktionärsdienste/IR, Publikationen
- **Schulung**, Instruktion, Weiterbildung
- Delikts- und **Betrugsbekämpfung**

Wem geben wir Personendaten bekannt?

- **Gruppengesellschaften** (vgl. Website)
- **Dienstleister** (die Ihre Daten teils in unserem Auftrag bearbeiten wie z.B. IT-Provider, teils in eigener Verantwortung bearbeiten wie z.B. Versicherungen)
- **Behörden** im In- und ggf. Ausland
- **Geschäftspartner** wie z.B. Lieferanten, Kunden, Marketing- und Projektpartner
- **Kreditauskunfteien**, die diese Daten bei sich für Bonitätsauskünfte speichern
- **Dritte**, die via Website/App Daten über Sie erheben (vgl. Liste auf der Website)[3]

Ihre Rechte?

Dazu gehört u.a. das **Auskunftsrecht**, das Recht auf Korrektur falscher Daten und ein Widerspruchsrecht. Schreiben Sie uns!

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

Was wichtig ist

- Führen Sie Ihre **Auftragsbearbeitungsverträge** (AVV) nach
  - Überall dort, wo jemand als Auftragsbearbeiter tätig ist
  - DSGVO-Verträge können nicht einfach übernommen werden
- **Darum ist das wichtig:**
  - Auftragsbearbeitungen kommen häufig vor, aber ebenso oft fehlen korrekte AVVs in der Schweiz noch
  - Fehlender / unvollständiger AVV ist strafbar (für den Verantwortliche)
- **Abgrenzen:** Verträge zwischen Verantwortlichen
  - Sind in der Schweiz nicht zwingend, aber zu empfehlen

Was (weiterhin) wichtig ist

- **Informationssicherheit!**
  - Schutz vor Angreifern durch geeignete technische und organisatorische Massnahmen
  - Plan für die Reaktion im Notfall (inkl. Kontakte)
  - Plan für die Geschäftsfortführung im Notfall
- **Darum ist das wichtig:**
  - Ihr Geschäft, der Schutz der ihnen anvertrauten Daten und Ihre Reputation hängt davon ab
- **Neu:** Meldepflicht für Data Breaches mit hohem Risiko
  - Meldung an den EDÖB und ggf. auch an betroffene Personen

https://www.rosenthal.ch/downloads/ACC-Cyber-Attack-Cheat-Sheet.pdf

Was weniger prioritär ist

- **Bearbeitungsverzeichnis (ROPA)**
  - Ein Inventar Ihrer Datenbearbeitungen
  - Sinnvoll für den Überblick, zwingend ab 250 Mitarbeiter
- **Datenschutz-Folgenabschätzung (DSFA)**
  - Dokumentiert unerwünschte negative Folgen (und diesbezügliche Massnahmen) bei potenziell heiklen Datenbearbeitungen
- **Prozesse für Betroffenenrechte**
  - Auskunftsrecht, Löschrecht, Korrekturrecht, Datenherausgabe
  - Gibt es schon; in den meisten Betrieben ad-hoc gehandhabt
  - Gibt es jemanden, der sich drum kümmert und Bescheid weiss?

Einige häufige Irrtümer

- Nein, das revidierte Datenschutzgesetz schreibt weiterhin **keine Einwilligung** vor – auch nicht für Profiling und Cookies
- Nein, **Cloud-Lösungen** sind trotz US-Bezug weiterhin erlaubt
- Nein, betreffend **E-Mail-Verschlüsselung** ändert sich nichts, und mit **Privacy-by-Design** auch nicht wirklich etwas
- Nein, es muss nicht jede **Verletzung des Datenschutzes** nach Bern gemeldet werden, sondern nur Verletzungen der Datensicherheit und nur falls das Risiko für Betroffene hoch ist
- Nein, das **Recht auf Vergessen** ist weder neu noch absolut
- Nein, nicht alles, was **DSGVO-"konform"** ist genügt für das neue DSG (z.B. Datenschutzerklärung, Providerverträge nicht)
- Nein, ein **Datenschutzbeauftragter** ist i.d.R. keine Pflicht

Anders ist es unter der DSGVO und im EU-Cookie-Recht: In der EU braucht es für Datenbearbeitungen einen Rechtsgrund, und Marketing- und Tracking-Cookies und ähnliche Verfahren oft eine Einwilligung.

Es galt und gilt: Personendaten müssen gelöscht oder anonymisiert werden, sobald sie ihren erlaubten Zweck erfüllt haben

Zum Online-Marketing

- **Singularisierung identifiziert für sich noch nicht**
  - EU-Datenschutzbehörden wollen anonyme Web-Profile ("digitaler Fussabdruck") als personenbezogene Daten verstanden wissen
  - Widerspricht der EU-Rechtsprechung und Schweizer Praxis
  - Referenzdaten-Test: Prüfdatensatz kann mit Referenzdatensatz einer bekannten, realen Person eindeutig verknüpft werden
- **Google Analytics rechtskonform einsetzbar**
  - 7 Schritte (Einwilligung, europäischer Vertrag, TIA, Data Sharing Option = off, Signals = off, IP Anonymization, anonyme User ID)
  - Anleitung/Diskussion der Entscheide: https://bit.ly/3NaEAiS
- **IAB TCF Framework in der Schweiz umsetzbar**

Achtung: EU-ePrivacy-Regelungen (Cookies etc.) gelten auch bei nicht-personenbezogenen Daten

Hintergrund sind nicht Bedenken wegen Google, sondern weil die NSA Zugriffe angeblich abhört

Und das Strafrecht?

- **Bussen** bei vorsätzlichen Verstössen neu bis CHF 250k
  - Sie müssen persönlich bezahlt werden (nicht versicherbar)
  - Für ungenügende DSE und Providerverträge, fehlender Schutz beim Datenexport in "unsichere" Drittländer, fehlende minimale Datensicherheit, falsche oder unvollständige Auskünfte an Betroffene, Verrat von vertraulichen beruflichen Personendaten
- **Gebüsst wird** auf Antrag wer (eventual-)vorsätzlich
  - gegen die Vorgaben verstösst
  - Verstösse nicht verhindert oder beseitigt, obwohl dies seine Aufgabe wäre (immer der Verwaltungsrat, aber z.B. auch die GL und jene Stellen, an welche die Verantwortung delegiert wurde)
  - Aber: Wer delegiert muss weiterhin überwachen

Büssen tut nicht der EDÖB, sondern die kantonalen Behörden; der EDÖB kann aber Datenbearbeitungen untersuchen und neu auch verbieten

Die Anforderungen an Datentransfers in Länder ausserhalb des EWR und von UK sind derzeit nicht sinnvoll umsetzbar. 2023 löst sich das vermutlich was die USA betrifft ("TADPF").

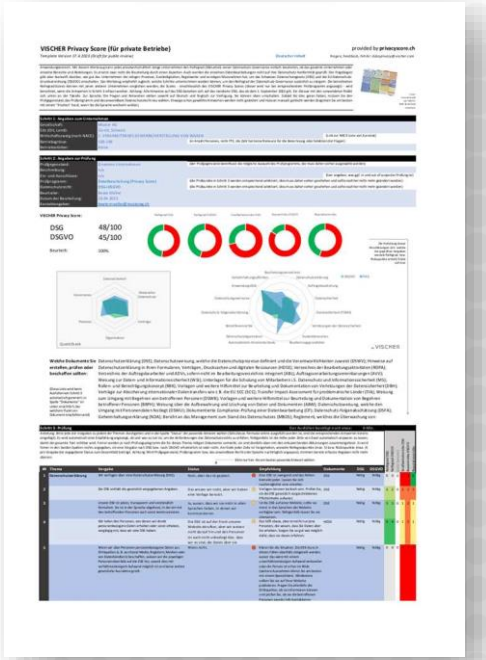
Das ganze Compliance-Programm auf einer Seite.

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

Ermitteln Sie Ihren VISCHER Privacy Score

- **Tool** (Online, Excel), welches Ihre Fitness für das neue DSG (und DSGVO) beurteilt und dokumentiert
  - Diverse **Prüfprogramme** (Prüfprogramm für kleine Betriebe von 20 Minuten, Detailprüfung 60 Minuten)
  - Sie erhalten einen **Bericht als PDF**, inkl. konkreten Handlungsempfehlungen
  - Dient auch als **Reporting** für VR und GL
  - Online-Version ist **kostenlos** und kann ohne Registrierung benutzt werden
  - Jetzt im öffentlichen **Testlauf** – probieren Sie VPS für sich selbst aus:

    privacyscore.ch



VISCHER

Danke für Ihre Aufmerksamkeit!

drosenthal@vischer.com, ram@vischer.com

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