

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?

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**

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

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 DSGVO-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



<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

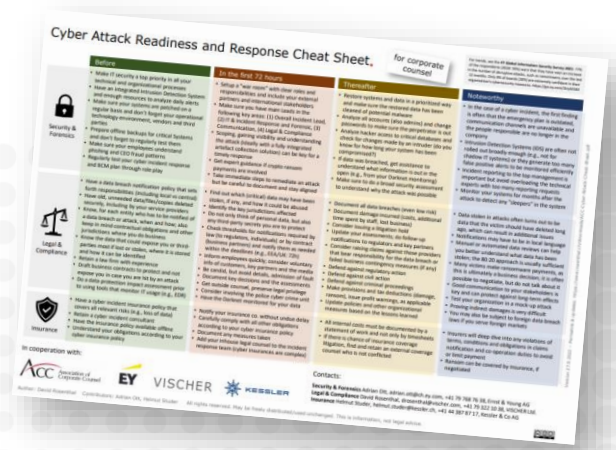
Was (weiterhin) wichtig ist

- **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").


revDSG – was zu tun ist

Für KMU Umgesetzt:
 • Neu ab 1.9.2023


10 Gebote zum Umgang mit Personendaten nach DSG¹

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 Daten²** 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


3. 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 Daten⁵ in grossem Umfang bearbeiten oder Hochrisiko-Profilung betreiben. 


4. 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 Bezug von Dritten vorab zu genehmigen⁶ (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 Länder⁵. 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 EU⁵ mit CH-Anpassung und keinen Grund zur Annahme haben, dass es zu problematischen Behördenzugriffen kommt (→ TIA machen!)
Wir prüfen unsere Verträge daraufhin! 


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 wir 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.⁷ In bestimmten Fällen müssen wir Personendaten, die wir erhalten und als Historie haben, den Personen zugesetzt Weitverwendung **herausgeben**.
Wir stellen sicher, dass wir das können!

7. Datenschutz Folgenabschätzung (DSFA)⁸

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. 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 Daten², 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 Daten² Bearbeitungsreglement.
Meldepflicht: Ist die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten verletzt **und** das Risiko negativer Folgen für einzelne Personen hoch (nicht bloss lästig) → EDOB melden (Formular auf <https://edob.admin.ch>) und für 2 Jahre dokumentieren; können sich Personen selbst vor Folgen schützen → Meldung auch an sie.
Jeder ist für Sicherheit mitverantwortlich! 

10. Wir verlassen uns nicht auf Einwilligungen

Wir stützen uns grundsätzlich nicht auf **Einwilligungen**. Falls doch, müssen sie **informiert** und **freiwillig** erfolgen, bei **sensitiven Daten²** und Hochrisiko-Profilung explizit. 

9. Kleines Berufsgeheimnis

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 ...

- ... 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!

Fragen?

IFAG auf <https://bit.ly/3R6G6t1> und mehr auf <https://bit.ly/38Cm2qJ>

Intern:

Extern:

Legende:  Intern  Extern  Datenschutz  Priorisierung  Umgesetzt

¹ revDSG/DSV: <https://datenrecht.ch/#gesetztexte>
² Besonders schützenswerte Daten: Art. 5 Bst. c revDSG
³ Vgl. Musterdatenschutzerklärung auf <https://dsat.ch>
⁴ Vorlagen: <https://dsat.ch>, <https://bit.ly/3zrgp0b>
⁵ Vgl. Anhang I der DSV (<https://bit.ly/3Dm3d9w>)
⁶ Vgl. FAQ (mit Bezugsquellen): <https://bit.ly/3zq6V2Z>
⁷ Vgl. TIA: <https://bit.ly/3L3mXf0> (mit Verweis auf FAQ)

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 DSGVO (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](https://www.privacyscore.ch)

The screenshot displays the VISCHER Privacy Score (VPS) tool interface. At the top, it reads 'VISCHER Privacy Score (für private Betriebe)'. Below this, there is a section titled 'Wichtigste Hinweise' with a red warning icon, followed by a 'VPS Score' section showing a score of 48/100 for DSGVO. The interface also features a 'Prüfung' section with a table of 10 items, each with a status indicator (green, yellow, or red).

Prüfung	Ergebnis	Anzahl	Punkte	Status
1. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
2. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
3. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
4. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
5. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
6. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
7. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
8. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
9. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green
10. Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn sie auf einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen beruht.	Ja	1	10	Green

VISCHER

Danke für Ihre Aufmerksamkeit!

drosenthal@vischer.com, ram@vischer.com

Zürich

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

www.vischer.com

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

