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!

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!

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.

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!

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.

Wir haben eine Stelle, die weiss was zu tun ist, wenn … 6 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/3qvGJZS
[7] Vgl. TIA: https://bit.ly/3L3mxYO (mit Verweis auf FAQ)

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

Intern:

Extern: (ggf. kostenpflichtig)

Legende: Umgang mit Daten | Governance | Betroffenenrechte | Prozesse | Prio Umsetzung | ☐ Umgesetzt ja/nein

Strafbar

Hier ist das revDSG strenger als die DSGVO oder erfordert andere, inkompatible Abläufe.

Version 13.9.2022 – Updates: www.rosenthal.ch

Autor: David Rosenthal, drosenthal@vischer.com

by VISCHER