VISCHER

kibesuisse.

Einführung in das revidierte Schweizer Datenschutzgesetz

Lucian Hunger, Rechtsanwalt, VISCHER AG
16.08.2023

Welches Recht ist für mich relevant?

Öffentliche Institution (z.B. durch Gemeinde betriebene Kinderbetreuung)	
Anwendbares Recht	• Kantonales Datenschutzgesetz • Die Kantone und Gemeinden haben in der Regel eigene Vorgaben zum Datenschutz, welche eingehalten werden müssen. Diese sind von öffentlichen Institutionen anzuwenden.
Aufsicht	• Aufsicht durch kantonale und kommunale Datenschutzbehörden

Private Trägerschaft (z.B. Stiftung, Verein, GmbH, AG oder Einzelunternehmen)	
Anwendbares Recht	Je nach Kanton und Gemeinde ist eine unterschiedliche Ausgangslage möglich (siehe Tipp) Bei Datenbearbeitungen im Rahmen der Kinderbetreuung; a) Kinderbetreuung ist im Kanton/der Gemeinde eine öffentliche Aufgabe: Die private Trägerschaft gilt in diesem Bereich als öffentliches Organ und es kommt das kantonale Datenschutzrecht zur Anwendung b) Kinderbetreuung ist im Kanton/der Gemeinde keine öffentliche Aufgabe: Es gilt das Bundesgesetz über den Datenschutz • Sonstige Datenbearbeitungen (z.B. Arbeitnehmendedaten, Einkäufe, Werbung): Es gilt das Bundesgesetz über den Datenschutz.
Aufsicht	• Wenn das kantonale Datenschutzrecht anwendbar ist: kantonale und kommunale Datenschutzbehörden • Ansonsten: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)

Und wie sieht das mit der DSGVO aus?

Europäische Datenschutzgrundverordnung (DSGVO)	
Für Schweizer Anbietende	Für Schweizer Unternehmen ist die DSGVO nur anwendbar, wenn das Unternehmen • an Privatpersonen im europäischen Wirtschaftsraum (EWR) Waren oder Dienstleistungen anbietet, oder • das Verhalten von Privatpersonen im EWR beobachtet. Für Anbietende in der Schweiz wird die DSGVO in der Regel nicht anwendbar sein, ausser das Angebot ist explizit auch auf Personen im EWR (z.B. im Fürstentum Liechtenstein) ausgerichtet und wird so beworben.
Fürstentum Liechtenstein	Das Fürstentum Liechtenstein ist Mitglied des EWR und die DSGVO ist auf Anbietende im Fürstentum Lichtenstein anwendbar.

- Frage: Muss auf der Website erwähnt werden, dass sich «unser Angebot ausschliesslich an abgebende Eltern mit Aufenthaltsort in der Schweiz richtet»?

Das neue DSG

- Das neue Datenschutzgesetz und seine Verordnungen gelten ab 1. September 2023
  - Keine (relevante) Übergangsfrist
- Ähnlich wie die EU DSGVO, aber (glücklicherweise) keine Kopie
  - Pragmatischer und weniger formalistisch als das EU-Recht
  - Nur in wenigen Bereichen strenger als DSGVO
- Grundprinzipien bleiben die gleichen
  - Mehr Governance, mehr Information, Data-Breach-Meldepflicht
  - Mehr Bussen für vorsätzliche Verstösse (sie sind persönlich!)

Personendaten und deren Bearbeitung

- **Personendaten** sind alle Angaben, welche sich auf eine identifizierte oder identifizierbare Person beziehen
  - Direkt: Name, Telefonnummer, E-Mail-Adresse
  - Indirekt: "Geschäftsführerin bei Tagesfamilienorganisation X", "ein berühmter Deutscher Wimbledon Sieger, der im Gefängnis war"
  - Beispiele: HR-Daten, Patientendossier, Kontaktlisten, etc.
  - «Relativer» Ansatz bei der Frage, ob Personendaten vorliegen
- Als **Datenbearbeitung** gilt jeder Umgang mit personen-bezogenen Daten (z.B. beschaffen, speichern, aufbewahren, verwenden, verändern, weitergeben, archivieren, löschen)

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**

VISCHER

3. Die Grundlagen des Datenschutzes

3.1. Wann und wie dürfen Daten bearbeitet werden?

Abhängig davon, welches Datenschutzgesetz anwendbar ist, sind die Vorgaben dazu, wann und wie Daten bearbeitet werden dürfen, unterschiedlich. In diesem Kapitel werden die Grundlagen behandelt, wann und wie Daten bearbeitet werden dürfen.

Bearbeitungsgrundsätze

- Die Bearbeitungsgrundsätze **ändern sich nicht** mit dem nDSG:
  - Rechtmässigkeit und Treu und Glauben
  - Transparenz
  - Zweckbindung
  - Verhältnismässigkeit (in Bezug auf den Zweck)
  - Richtigkeit (in Bezug auf den Zweck)
  - Need-to-Know Prinzip
  - Datensicherheit
- Grundsätzlich ist **kein Rechtsgrund** nötig für eine Bearbeitung (≠ DSGVO)
  - Ausnahmen: (i) Verstoss gegen Bearbeitungsgrundsätze, (ii) Widerspruch der betroffenen Person, (iii) Bekanntgabe besonders schützenswerter Personendaten, (iv) Datenbearbeitung im Rahmen einer öffentlichen Aufgabe

Bild generiert von DALL-E, dem KI-Modell von OpenAI

Grundsätzlich gilt: Bisher erlaubte Bearbeitungen von Personendaten bleiben auch unter dem revDSG erlaubt

Rechtfertigung

- Einwilligung durch die betroffene Person
  - z.B. Publikation von Fotos
- Datenbearbeitung infolge einer gesetzlichen Vorgabe
  - z.B. Datenbekanntgabe an Behörde infolge gesetzlicher Pflicht
- Überwiegendes privates Interesse
  - Abschluss oder Abwicklung eines Vertrages
  - Kreditprüfung
  - Statistiken
  - Weitere in Art. 31 revDSG

Nur auf Einwilligung stützten, wenn keine andere Möglichkeit besteht oder die Bearbeitung sonst nicht zulässig wäre

Der grosse Unterschied bei öffentlichen Aufgaben

- Bei der Datenbearbeitung als öffentliches Organ dürfen Personendaten bearbeitet werden, wenn:
  - eine **gesetzliche Grundlage** besteht

  oder

  - die Bearbeitung der **Erfüllung einer gesetzlichen Aufgabe** dient

  und

  - die **Bearbeitungsgrundsätze** eingehalten werden

Bearbeiten Sie im Rahmen der Kinderbetreuung nur das für die Betreuung Notwendige.
Dies ist grundsätzlich nach kantonalem Recht sowie nach DSG/revDSG kein Problem.

VISCHER

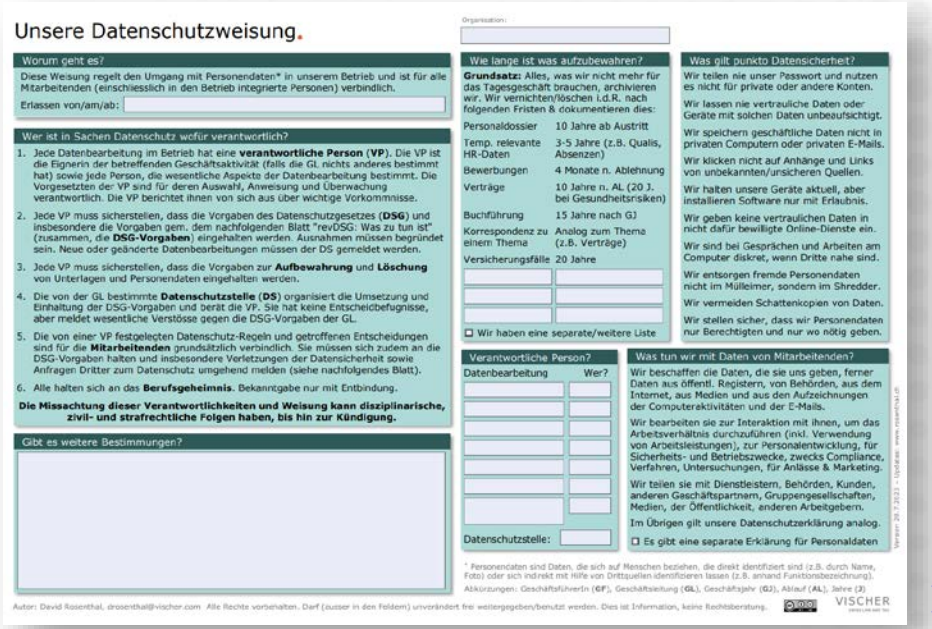

revDSG – was zu tun ist
Für KMU
Umgesetzt:
Neu ab 1.9.2023
Zehn Gebote zum Umgang mit Personendaten nach DSG[1]
1. Wir sagen der Person vorher, was wir mit ihren Daten wozu tun.
2. Wir halten uns daran und setzen Daten nicht zweckwidrig ein.
3. Wir üben uns in Datensparsamkeit und "need-to-know".
4. 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
10. Wir beschaffen Daten au
Ausnahmen sind (nur
Wir gestalten jede Date
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
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
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
Auftragsbearbeiter darf nur
uch tun dürfen (z.B. i.d.R.
tzung für sich). Wir prüfen
euen ADV auf Konformität.
Wenn Daten ins Ausland
Problemlos: EWR, UK, ange
Alle anderen Staaten u.a.
• Export zur Abwicklung eine
mit oder für die betroffene
• Expliziter Verzicht auf Schu
• Abschluss der "Standardve
EU[6] mit CH-Anpassung und
Annahme haben, dass es z
Behördenzugriffen kommt
Wir prüfen unsere Vertr
Privacy by Default
Wo wir in Apps, auf Websites etc. Einstellungen zum Datenschutz haben, sind diese auf das Minimum voreingestellt. Die Entwickler achten darauf.
tzung strafbar ist (bis CHF 250k, auf Antrag)
lten wir geheim oder
halten werden.
Die Daten sind sicher, son
Technisch: Zugang nur "ne
mit persönlichem Konto, "MF
Zugriff, Audit-Trails (ggf. Pfli
Daten[2], 1 Jahr), Pseudonymi
Antimalware-Software, Backu
Organisatorisch: Weisunge
Blatt dazu verwenden), Schu
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!
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!
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.
wenn ...
... 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?
(FAQ auf https://bit.ly/3RC49c1 und mehr auf https://bit.ly/3RCmuFQ)
Intern:
Extern:
(ggf. kostenpflichtig)
Legende:
Umgang mit Daten
Betroffenenrechte
Governance
Prozesse
Prio Umsetzung
Umgesetzt ja/nein
[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)
Hier ist das revDSG strenger als die DSGVO oder erfordert andere, inkompatible Abläufe.
Strafbar
Version 13.9.2022 – Updates: www.rosenthal.ch
Autor: David Rosenthal, drosenthal@vischer.com
Alle Rechte vorbehalten. Darf (ausser in den Feldern) unverändert frei weitergegeben/benutzt werden. Dies ist Information, keine Rechtsberatung.
„VISCHER
4. Wie soll ich die Vorgaben umsetzen und was muss ich denn nun machen?
Dieses Kapitel gibt Hilfestellung zur Umsetzung im Unternehmen und zeigt weitere Vorgaben auf, welche das Datenschutzgesetz neben den allgemeinen Grundsätzen vorschreibt. Im Anhang der Wegleitung finden Sie auch eine Checkliste, in welcher Reihenfolge Sie etwas umsetzen sollten.

Datenschutzperson / Datenschutzstelle

- Definieren einer zuständigen Person / Stelle
  - Ist nicht verantwortlich für die Datenbearbeitungen, sondern für die Umsetzung des Datenschutzes
  - Ansprechperson
  - Kümmert sich um die Datenschutzerklärung
  - Bearbeitet Betroffenenbegehren
  - Schult Mitarbeitende
  - Holt wenn nötig Unterstützung
- ≠ Datenschutzberater
- ≠ Datenschutzbeauftragter im Sinne der DSGVO

Weisung

- Erlassen Sie eine Weisung mit den wichtigsten Handlungsanweisungen



Unsere Datenschutzweisung.

Organisation:

Worum geht es?

Diese Weisung regelt den Umgang mit Personendaten* in unserem Betrieb und ist für alle Mitarbeitenden (einschliesslich in den Betrieb integrierte Personen) verbindlich.

Erlassen von/am/ab:

Wer ist in Sachen Datenschutz wofür verantwortlich?

1. Jede Datenbearbeitung im Betrieb hat eine **verantwortliche Person (VP)**. Die VP ist die Eignerin der betreffenden Geschäftsaktivität (falls die GL nichts anderes bestimmt hat) sowie jede Person, die wesentliche Aspekte der Datenbearbeitung bestimmt. Die Vorgesetzten der VP sind für deren Auswahl, Anweisung und Überwachung verantwortlich. Die VP berichtet ihnen von sich aus über wichtige Vorkommnisse.
2. Jede VP muss sicherstellen, dass die Vorgaben des Datenschutzgesetzes (**DSG**) und insbesondere die Vorgaben gem. dem nachfolgenden Blatt "revDSG: Was zu tun ist" (zusammen, die **DSG-Vorgaben**) eingehalten werden. Ausnahmen müssen begründet sein. Neue oder geänderte Datenbearbeitungen müssen der DS gemeldet werden.
3. Jede VP muss sicherstellen, dass die Vorgaben zur **Aufbewahrung** und **Löschung** von Unterlagen und Personendaten eingehalten werden.
4. Die von der GL bestimmte **Datenschutzstelle (DS)** organisiert die Umsetzung und Einhaltung der DSG-Vorgaben und berät die VP. Sie hat keine Entscheidbefugnisse, aber meldet wesentliche Verstösse gegen die DSG-Vorgaben der GL.
5. Die von einer VP festgelegten Datenschutz-Regeln und getroffenen Entscheidungen sind für die **Mitarbeitenden** grundsätzlich verbindlich. Sie müssen sich zudem an die DSG-Vorgaben halten und insbesondere Verletzungen der Datensicherheit sowie Anfragen Dritter zum Datenschutz umgehend melden (siehe nachfolgendes Blatt).
6. Alle halten sich an das **Berufsgeheimnis**. Bekanntgabe nur mit Entbindung.

Die Missachtung dieser Verantwortlichkeiten und Weisung kann disziplinarische, zivil- und strafrechtliche Folgen haben, bis hin zur Kündigung.

Gibt es weitere Bestimmungen?

Wie lange ist was aufzubewahren?

Grundsatz: Alles, was wir nicht mehr für das Tagesgeschäft brauchen, archivieren wir. Wir vernichten/löschen i.d.R. nach folgenden Fristen & dokumentieren dies:

Personaldossier	10 Jahre ab Austritt
Temp. relevante HR-Daten	3-5 Jahre (z.B. Qualis, Absenzen)
Bewerbungen	4 Monate n. Ablehnung
Verträge	10 Jahre n. AL (20 J. bei Gesundheitsrisiken)
Buchführung	15 Jahre nach GJ
Korrespondenz zu einem Thema	Analog zum Thema (z.B. Verträge)
Versicherungsfälle	20 Jahre

☐ Wir haben eine separate/weitere Liste

Was gilt punkto Datensicherheit?

Wir teilen nie unser Passwort und nutzen es nicht für private oder andere Konten.

Wir lassen nie vertrauliche Daten oder Geräte mit solchen Daten unbeaufsichtigt.

Wir speichern geschäftliche Daten nicht in privaten Computern oder privaten E-Mails.

Wir klicken nicht auf Anhänge und Links von unbekannten/unsicheren Quellen.

Wir halten unsere Geräte aktuell, aber installieren Software nur mit Erlaubnis.

Wir geben keine vertraulichen Daten in nicht dafür bewilligte Online-Dienste ein.

Wir sind bei Gesprächen und Arbeiten am Computer diskret, wenn Dritte nahe sind.

Wir entsorgen fremde Personendaten nicht im Mülleimer, sondern im Shredder.

Wir vermeiden Schattenkopien von Daten.

Wir stellen sicher, dass wir Personendaten nur Berechtigten und nur wo nötig geben.

Verantwortliche Person?

Datenbearbeitung	Wer?

Datenschutzstelle:

Was tun wir mit Daten von Mitarbeitenden?

Wir beschaffen die Daten, die sie uns geben, ferner Daten aus öffent. Registern, von Behörden, aus dem Internet, aus Medien und aus den Aufzeichnungen der Computeraktivitäten und der E-Mails.

Wir bearbeiten sie zur Interaktion mit ihnen, um das Arbeitsverhältnis durchzuführen (inkl. Verwendung von Arbeitsleistungen), zur Personalentwicklung, für Sicherheits- und Betriebszwecke, zwecks Compliance, Verfahren, Untersuchungen, für Anlässe & Marketing.

Wir teilen sie mit Dienstleistern, Behörden, Kunden, anderen Geschäftspartnern, Gruppengesellschaften, Medien, der Öffentlichkeit, anderen Arbeitgebern.

Im Übrigen gilt unsere Datenschutzerklärung analog.

☐ Es gibt eine separate Erklärung für Personaldaten

* Personendaten sind Daten, die sich auf Menschen beziehen, die direkt identifiziert sind (z.B. durch Name, Foto) oder sich indirekt mit Hilfe von Drittquellen identifizieren lassen (z.B. anhand Funktionsbezeichnung).

Abkürzungen: Geschäftsführer/in (GF), Geschäftsleitung (GL), Geschäftsjahr (GJ), Ablauf (AL), Jahre (J)

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

Version 26.7.2023 – Updates: www.rosenthal.ch

VISCHER

https://www.rosenthal.ch/downloads/VISCHER-DSG-Weisung-KMU.pdf

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 Quel

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 [illegible] und worauf [illegible][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.

4.2.1. Das Bearbeitungsverzeichnis

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!

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.

[illegible] Folgenabschätzung (DSFA)

[illegible] Datenbearbeitung für Betroffene [illegible] machen wir eine DSFA. Darin dok[illegible] Vorhaben und die Massnahmen [illegible] 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** [illegible] Datenschutz haben, [illegible] f das **Mini-** [illegible] gestellt. Die Entwick[illegible] chten 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 … 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!

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

Intern:

Extern: (ggf. kostenpflichtig)

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

[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)

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

Version 13.9.2022 – Updates: www.rosenthal.ch

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

„VISCHER

Inventar der Bearbeitungen / Bearbeitungsverzeichnis

- "Inventar" aller Aktivitäten in der Unternehmung, welche Bearbeitungen von Personendaten betreffen (aktuell zu halten)
- Ausnahme für KMU (<250 Mitarbeiter, wenn Risiko der Bearbeitungen gering)
  - keine Ausnahme u.a. bei Bearbeitung von Gesundheitsdaten in grossem Umfang
- kann hilfreich bzw. eine Chance sein

Mindestangaben nach Art. 12 revDSG

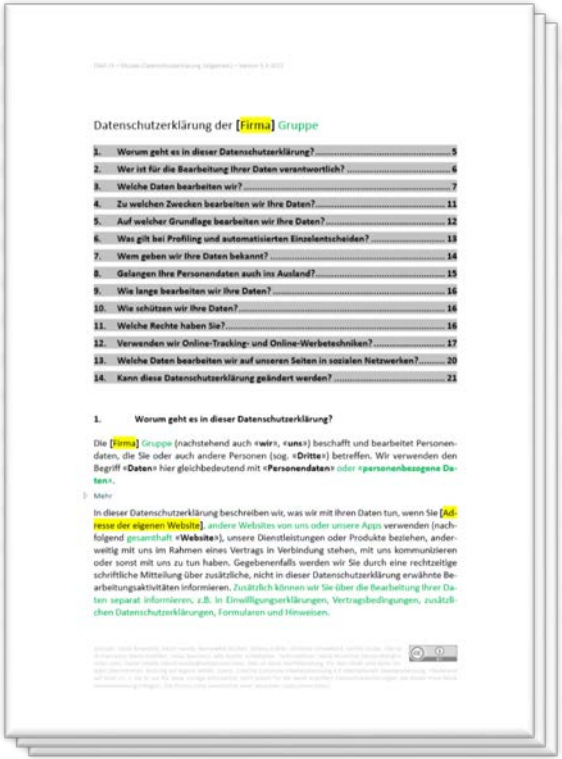
- Identität des/der Verantwortlichen
- Bearbeitungszweck
- Kategorien betroffener Personen
- Kategorien von Personendaten
- Kategorien der Empfänger
- Aufbewahrungsdauer (mindestens Kriterien zu deren Festlegung)
- Details betr. Bekanntgabe ins Ausland (Staaten und Garantien für Übermittlung in unsichere Drittstaaten)
- Massnahmen zur Datensicherheit


revDSG – was zu tun ist
Für KMU
Umgesetzt:
Neu ab 1.9.2023
4.2.2. Datenschutzerklärung (DSE)
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 "bess ... Grund möglich.
Wir gestalten jede Datenbearbeit...
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!
Wir ge...
Wir identifizieren die Person...
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)
...kto Datenbearbeitung für ...cher sein könnten, machen wir eine DSF... ...kumentieren 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 / Prio Umsetzung / Betroffenenrechte / Prozesse / Umgesetzt ja/nein
Hier ist das revDSG strenger als die DSGVO oder erfordert andere, inkompatible Abläufe. Strafbar
Version 13.9.2022 – Updates: www.rosenthal.ch
Autor: David Rosenthal, drosenthal@vischer.com Alle Rechte vorbehalten. Darf (ausser in den Feldern) unverändert frei weitergegeben/benutzt werden. Dies ist Information, keine Rechtsberatung.
„VISCHER

Datenschutzerklärung

- Informationspflicht des Verantwortlichen bei der Beschaffung von Personendaten
  - generelle Informationspflicht
- Allgemeine Datenschutzerklärung (DSE) als bewährter Ansatz
  - Spezielle DSE für Datenbearbeitungen, die nicht von der allgemeinen DSE abgedeckt sind
- Ausnahmen von der Informationspflicht gemäss Art. 20 nDSG (z.B. wenn die Datenbearbeitung gesetzlich vorgesehen ist)

Wird der Mindestinhalt nicht abgedeckt, kann dies strafbar sein.



Datenschutzerklärung der [Firma] Gruppe

1. Worum geht es in dieser Datenschutzerklärung?

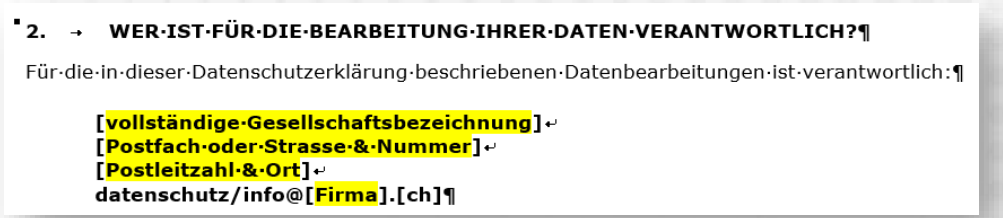
Die [Firma] Gruppe (nachstehend auch «wir», «uns») beschafft und bearbeitet Personendaten, die Sie oder auch andere Personen (sog. «Dritte») betreffen. Wir verwenden den Begriff «Daten» hier gleichbedeutend mit «Personendaten» oder «personenbezogene Daten».

Mehr

In dieser Datenschutzerklärung beschreiben wir, was wir mit Ihren Daten tun, wenn Sie [Adresse der eigenen Website], andere Websites von uns oder unsere Apps verwenden (nachfolgend gesamthaft «Website»), unsere Dienstleistungen oder Produkte beziehen, anderweitig mit uns im Rahmen eines Vertrags in Verbindung stehen, mit uns kommunizieren oder sonst mit uns zu tun haben. Gegebenenfalls werden wir Sie durch eine rechtzeitige schriftliche Mitteilung über zusätzliche, nicht in dieser Datenschutzerklärung erwähnte Bearbeitungsaktivitäten informieren. Zusätzlich können wir Sie über die Bearbeitung Ihrer Daten separat informieren, z.B. in Einwilligungserklärungen, Vertragsbedingungen, zusätzlichen Datenschutzerklärungen, Formularen und Hinweisen.

kibesuisse Muster Datenschutzerklärung

- Mindestinhalt in Art. 19 revDSG
  - Identität des Verantwortlichen

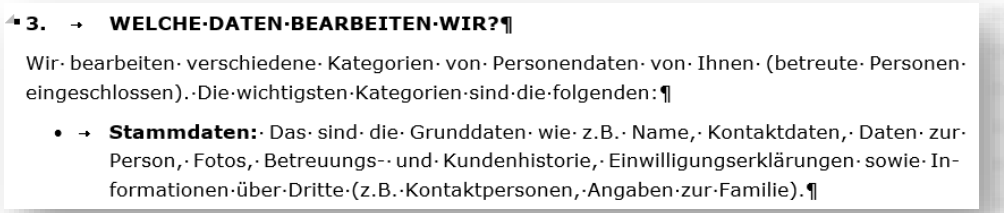


2. → WER·IST·FÜR·DIE·BEARBEITUNG·IHRER·DATEN·VERANTWORTLICH?¶

Für·die·in·dieser·Datenschutzerklärung·beschriebenen·Datenbearbeitungen·ist·verantwortlich:¶

[vollständige·Gesellschaftsbezeichnung]↵
[Postfach·oder·Strasse·&·Nummer]↵
[Postleitzahl·&·Ort]↵
datenschutz/info@[Firma].[ch]¶

  - Kategorien der Personendaten, die nicht bei der betroffenen Person erhoben werden



3. → WELCHE·DATEN·BEARBEITEN·WIR?¶

Wir· bearbeiten· verschiedene· Kategorien· von· Personendaten· von· Ihnen· (betreute· Personen· eingeschlossen).·Die·wichtigsten·Kategorien·sind·die·folgenden:¶

- → **Stammdaten:**· Das· sind· die· Grunddaten· wie· z.B.· Name,· Kontaktdaten,· Daten· zur· Person,· Fotos,· Betreuungs-· und· Kundenhistorie,· Einwilligungserklärungen· sowie· Informationen·über·Dritte·(z.B.·Kontaktpersonen,·Angaben·zur·Familie).¶

kibesuisse Muster Datenschutzerklärung

- Mindestinhalt in Art. 19 revDSG
  - Bearbeitungszwecke

5. → ZU·WELCHEN·ZWECKEN·BEARBEITEN·WIR·IHRE·DATEN?¶

- → **Kommunikation:**·Um·mit·Ihnen·kommunizieren·zu·können·(z.B.·zur·Beantwortung·von·Anfragen,·der·Vertragsabwicklung·und·der·Betreuung),·bearbeiten·wir·Daten·von·Ihnen.¶

  - Kategorien von Empfängern

6. WEM GEBEN WIR IHRE DATEN BEKANNT?

Im Zusammenhang mit unseren Verträgen, der Website, unseren Dienstleistungen, unseren rechtlichen Pflichten oder sonst zur Wahrung unserer berechtigten Interessen und den weiteren in Ziff. 5 aufgeführten Zwecken, übermitteln wir Ihre Personendaten auch an Dritte, insbesondere an die folgenden Kategorien von Empfängern:

- **Gruppengesellschaften:** […]
- **Dienstleister:** […]
- **Vertragspartner, inklusive Eltern und betreute Personen:** […]
- **Behörden:** […]
- **Weitere Personen:** […]

kibesuisse Muster Datenschutzerklärung

- Mindestinhalt in Art. 19 revDSG
  - Angaben zur Bekanntgabe ins Ausland
    - Alle Länder nennen, nicht nur jene ausserhalb des EWR (Länder müssen bestimmbar sein; z.B.: «alle Länder der Welt»
    - Garantien und Ausnahmen nennen

7. GELANGEN IHRE PERSONENDATEN AUCH INS AUSLAND?

Wir bearbeiten und speichern Personendaten hauptsächlich in der Schweiz und im Europäischen Wirtschaftsraum (EWR), im Ausnahmefall – beispielsweise über Unterauftragsbearbeiter unserer Dienstleister – aber potentiell 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 (…).

Cookies und Website-Plugins

- Das Schweizer Recht schreibt keinen Cookie-Banner und keine Einwilligung für die Nutzung von Cookies vor - Information und Widerspruchsmöglichkeit reicht aus

10. WIE BEARBEITEN WIR DATEN IM ZUSAMMENHANG MIT UNSERER WEBSITE UND ÜBRIGEN DIGITALEN DIENSTEN?

Bei der Nutzung unserer Website (inkl. Newsletter und weitere digitale Angebote) fallen Daten an, die in Protokollen gespeichert werden (insbesondere technische Daten). Zudem können wir Cookies und ähnliche Techniken (z.B. Pixel-Tags oder Fingerprints) einsetzen, um Website-Besucher wiederzuerkennen, ihr Verhalten aufzuzeichnen und Präferenzen zu erkennen. Ein Cookie ist eine kleine Datei, die zwischen dem Server und Ihrem System übermittelt wird und ermöglicht die Wiedererkennung eines bestimmten Geräts oder Browsers.

Sie können Ihren Browser so einstellen, dass dieser Cookies automatisch ablehnt, akzeptiert oder löscht. Sie können auch Cookies im Einzelfall deaktivieren oder löschen. Wie Sie die Cookies in Ihrem Browser verwalten können, erfahren Sie im Hilfemenü Ihres Browsers.

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.

- Nennen Sie Dritte, die über Software und Dienste für ihre eigenen Zwecke Daten über Nutzer sammeln (Name, Sitz, Hinweis auf deren DSE), z.B. über separate Liste

Fragen?

- Weshalb sind die Microsoft Produkte in der Datenschutzerklärung nicht aufgeführt?

6. WEM GEBEN WIR IHRE DATEN BEKANNT?

Im Zusammenhang mit unseren Verträgen, der Website, unseren Dienstleistungen, unseren rechtlichen Pflichten oder sonst zur Wahrung unserer berechtigten Interessen und den weiteren in Ziff. 5 aufgeführten Zwecken, übermitteln wir Ihre Personendaten auch an Dritte, insbesondere an die folgenden Kategorien von Empfängern:

- **Gruppengesellschaften:** […]
- **Dienstleister:** […]
- **Vertragspartner, inklusive Eltern und betreute Personen:** […]
- **Behörden:** […]
- **Weitere Personen:** […]

- **Dienstleister:** Wir arbeiten mit Dienstleistern im In- und Ausland zusammen, die (i) in unserem Auftrag, (ii) in gemeinsamer Verantwortung mit uns oder (iii) in eigener Verantwortung Daten bearbeiten (z.B. IT-Provider, Banken, Versicherungen). Dazu können auch Gesundheitsdaten gehören.

VISCHER

revDSG – was zu tun ist

Für KMU · Umgesetzt: ☐ · Neu ab 1.9.2023

4.2.3. Auskunft-, Korrekturrecht (Betroffenenrechte)

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** …
10. Wir beschaffen Daten auf **legale Weise** …

Ausnahmen sind … **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 … (Zweck), 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 Personendaten 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 … 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 … 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 · Betroffenenrechte · Governance · Prozesse · Prio Umsetzung · Umgesetzt ja/nein

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

Version 13.9.2022 – Updates: www.rosenthal.ch

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

„VISCHER

Auskunft-, Korrekturrecht (Betroffenenrechte)

- Verantwortlichkeit vorsehen
- Auskunftsrecht
  - Muss innert 30 Tagen erfolgen
  - Muss grundsätzlich kostenlos erfolgen
  - Auskünfte können teilweise oder vollständig verweigert werden, z.B. zum
    - Schutz von anderen Personen (mit einer Auskunft dürfen keine Personendaten anderer bekanntgegeben werden.)
    - Schutz von Geschäftsgeheimnissen
- Recht auf Korrektur von Daten
- Recht auf Löschung

4.2.4. Datenbekanntgabe ins Ausland

Datenbekanntgabe ins Ausland

- Daten dürfen ins Ausland bekannt gegeben werden, wenn entweder
  - das Land über angemessenen Datenschutz verfügt (z.B. EWR, (noch) nicht USA)

  oder
  - zusätzliche Schutzmassnahmen wie vertragliche Vereinbarungen (Standardvertragsklauseln) getroffen wurden

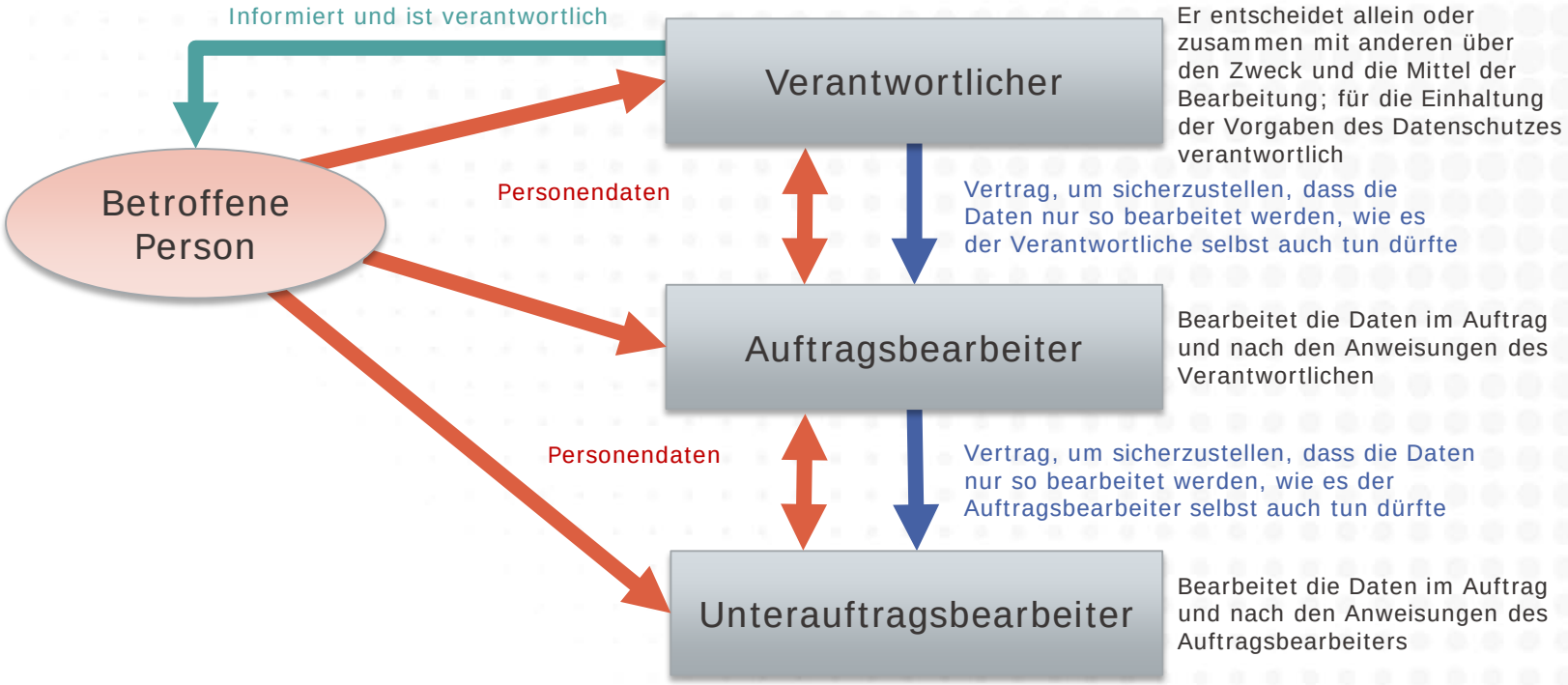
  oder
  - eine Ausnahme vorliegt (z.B. Einwilligung)
- Nicht nur ein aktives Senden, sondern auch der Fernzugriff ist eine Bekanntgabe

Werden Daten in ein Land bekannt gegeben, ohne die oben genannten Voraussetzungen zu erfüllen, kann dies strafbar sein.

VISCHER

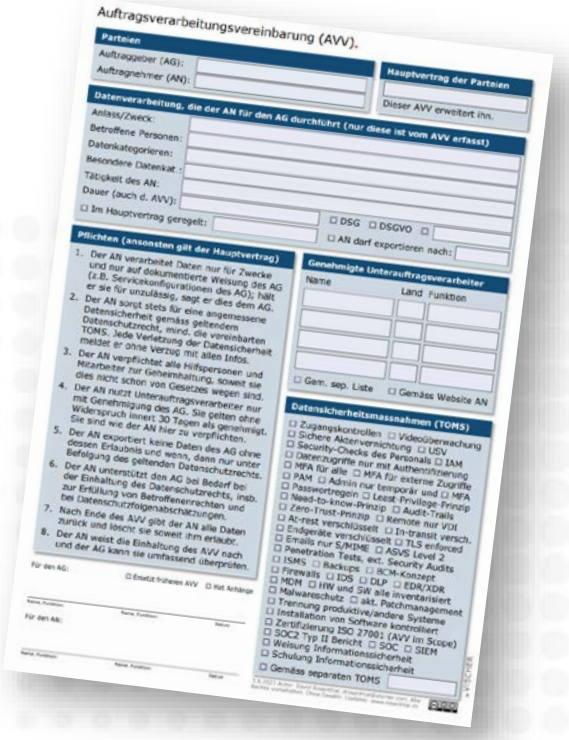

revDSG – was zu tun ist
Für KMU
Umgesetzt:
Neu ab 1.9.2023
4.2.5. Auftragsbearbeitung
7 Zehn Gebote zum Umgang mit Personendaten nach DSG[1]
1. Wir sagen der Person vorher, was wir mit ihren Daten wozu tun.
2. Wir halten uns daran und setzen Daten nicht zweckwidrig ein.
3. Wir üben uns in Datensparsamkeit 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 / Regionen sie gehen / wir uns re
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
sem Umfang bearbeiten oder
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!
8 Privacy by Default
Bei Vorhaben, [illegible] Betroffene risikoreicher sein k[illegible] 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.
zum Daten[illegible] sind also 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
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.
„VISCHER

Rollen bei einer Datenbearbeitung



Auftragsbearbeitungsvertrag

- Schliessen Sie einen Auftragsbearbeitungsvertrag ab
- Mindestinhalt
  - Pflicht des Auftragsbearbeiters nur aufgrund dokumentierter Weisung des Verantwortlichen Daten zu bearbeiten
  - Recht des Verantwortlichen die Datenbearbeitung zu prüfen
  - Pflicht des Auftragsbearbeiters Daten zurückzugeben und zu löschen
  - Regelung über Beizung von Unterauftragsbearbeiter
  - Unterstützungspflichten bei der Einhaltung des DSG
- Auftragsbearbeitungsvertrag auf einer Seite


Auftragsverarbeitungsvereinbarung (AVV).

Parteien

Auftraggeber (AG):

Auftragnehmer (AN):

Hauptvertrag der Parteien

Dieser AVV erweitert ihn.

Datenverarbeitung, die der AN für den AG durchführt (nur diese ist vom AVV erfasst)

Anlass/Zweck:

Betroffene Personen:

Datenkategorien:

Besondere Datenkat.:

Tätigkeit des AN:

Dauer (auch d. AVV):

☐ Im Hauptvertrag geregelt:

☐ DSG ☐ DSGVO ☐

☐ AN darf exportieren nach:

Pflichten (ansonsten gilt der Hauptvertrag)

1. Der AN verarbeitet Daten nur für Zwecke und nur auf dokumentierte Weisung des AG (z.B. Servicekonfigurationen des AG); hält er sie für unzulässig, sagt er dies dem AG.
2. Der AN sorgt stets für eine angemessene Datensicherheit gemäss geltendem Datenschutzrecht, mind. die vereinbarten TOMS. Jede Verletzung der Datensicherheit meldet er ohne Verzug mit allen Infos.
3. Der AN verpflichtet alle Hilfspersonen und Mitarbeiter zur Geheimhaltung, soweit sie dies nicht schon von Gesetzes wegen sind.
4. Der AN nutzt Unterauftragsverarbeiter nur mit Genehmigung des AG. Sie gelten ohne Widerspruch binnen 30 Tagen als genehmigt. Sie sind wie der AN hier zu verpflichten.
5. Der AN exportiert keine Daten des AG ohne dessen Erlaubnis und wenn, dann nur unter Befolgung des geltenden Datenschutzrechts.
6. Der AN unterstützt den AG bei Bedarf bei der Einhaltung des Datenschutzrechts, insb. zur Erfüllung von Betroffenenrechten und bei Datenschutzfolgenabschätzungen.
7. Nach Ende des AVV gibt der AN alle Daten zurück und löscht sie soweit ihm erlaubt.
8. Der AN weist die Einhaltung des AVV nach und der AG kann sie umfassend überprüfen.

Genehmigte Unterauftragsverarbeiter

Name | Land | Funktion

☐ Gem. sep. Liste ☐ Gemäss Website AN

Datensicherheitsmassnahmen (TOMS)

☐ Zugangskontrollen ☐ Videoüberwachung
☐ Sichere Aktenvernichtung ☐ USV
☐ Security-Checks des Personals ☐ IAM
☐ Datenzugriffe nur mit Authentifizierung
☐ MFA für alle ☐ MFA für externe Zugriffe
☐ PAM ☐ Admin nur temporär und ☐ MFA
☐ Passwortregeln ☐ Least-Privilege-Prinzip
☐ Need-to-know-Prinzip ☐ Audit-Trails
☐ Zero-Trust-Prinzip ☐ Remote nur VDI
☐ At-rest verschlüsselt ☐ In-transit versch.
☐ Endgeräte verschlüsselt ☐ In-transit versch.
☐ Emails nur S/MIME ☐ TLS enforced
☐ Penetration Tests, ext. Security Audits
☐ ISMS ☐ Backups ☐ BCM-Konzept
☐ Firewalls ☐ IDS ☐ DLP ☐ EDR/XDR
☐ MDM ☐ HW und SW alle inventarisiert
☐ Malwareschutz ☐ akt. Patchmanagement
☐ Trennung produktive/andere Systeme
☐ Installation von Software kontrolliert
☐ Zertifizierung ISO 27001 (AVV im Scope)
☐ SOC2 Typ II Bericht ☐ SOC ☐ SIEM
☐ Weisung Informationssicherheit
☐ Schulung Informationssicherheit
☐ Gemäss separaten TOMS

Für den AG: ☐ Ersetzt früheren AVV ☐ Hat Anhänge

Für den AN:

Das Hinzuziehen eines Auftragsbearbeiters oder einer Auftragsbearbeiterin ohne Vertrag kann bestraft werden.

Und dürfen wir die Cloud nutzen?

- **Ja**, das neue DSG **erlaubt** den Einsatz der **Cloud** weiterhin
  - Datenschützer kritisieren die Cloud vor allem wegen den USA
- **Faustregeln** (siehe Netzwoche https://bit.ly/429W6ZB)
  - **Keine** Nutzung von **Diensten für Private**
  - Wähle einen Provider mit **Sitz im EWR oder Schweiz** und mit **Speicherung der Daten im EWR oder der Schweiz**
  - Schliesse mit dem Provider einen **Auftragsbearbeitungsvertrag** ab
  - Aktiviere im Falle von besonders heikler Daten wenn möglich die **Option**, dass der Provider **vor einem Datenzugriff fragen muss**
  - Verstehe, wie ein Cloud-Dienst **sicher zu konfigurieren** ist
  - Sichere die Daten **ausserhalb der Cloud** (Provider sichern nicht)
  - Habe einen **Exit-Plan** für den Fall, dass die Cloud ausfällt

VISCHER

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

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 [illegible] worauf [illegible][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.

4.2.7. Datenlöschung

5 Wenn Daten in [illegible] gewähren Betroffenen ihre Rechte

Problemlos: EW[illegible] 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!

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 · Betroffenenrechte · Governance · Prozesse · Prio Umsetzung · ☐ Umgesetzt ja/nein

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

Version 13.9.2022 – Updates: www.rosenthal.ch

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

„VISCHER

Wie lange dürfen Daten aufbewahrt werden?

- Personendaten müssen gelöscht oder anonymisiert werden, sobald sie für den Zweck der Bearbeitung nicht mehr erforderlich sind und keine Aufbewahrungspflicht besteht
- Beispiele
  - Buchungsbelege: Steuerjahr + 10 Jahre
  - (Betreuungs-)Verträge: Vertragsende + 10 Jahre
  - Erfolglose Bewerber: Ablehnung + 4 Monate
  - Mitarbeiterdaten: Vertragsende + 10 Jahre
  - Dokumentation zum Betreuungsverlauf / Gesprächsprotokolle: Unterschiede nach kantonalem Recht

VISCHER


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
4.2.8. Datensicherheit
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. Datenschutz- Zwecke sind nicht geschützt. Wir schützen Geschäftsgeheimnisse.
gen. Ist lies.
Jede Person kann Lösc 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 ... 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 / Betroffenenrechte / Governance / Prozesse / 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.
VISCHER

Datensicherheit

- Die Sicherheit der Personendaten muss jederzeit in angemessener Weise gewährleistet sein. Sicherheit bedeutet Vertraulichkeit, Integrität und Verfügbarkeit der Daten, d.h. ihr Schutz vor unbefugtem Zugang, vor ihrer Manipulation oder unerwünschter Veränderung und vor Verlust.
  - Achten Sie darauf, dass Ihre IT-Infrastruktur auf dem neusten Stand ist.
  - Lassen Sie die Datensicherheit von Spezialisten sicherstellen.
  - Erstellen Sie Backups (auch wenn Sie die Cloud nutzen).
  - Schulen Sie Ihre Mitarbeitenden im Umgang mit der IT.

Mangelnde Datensicherheit kann strafbar sein. Nicht jede Datensicherheitsverletzung ist strafbar, aber der aktuelle technische Minimalstandard ist einzuhalten.

VISCHER

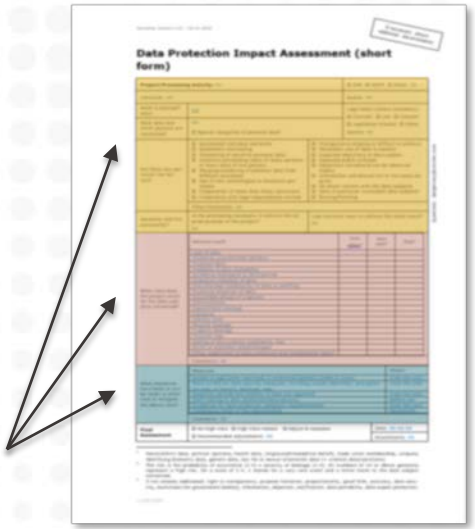

revDSG – was zu tun ist.
Für KMU
Umgesetzt:
Neu ab 1.9.2023
7 Zehn Gebote zum Umgang mit Personendaten nach DSG[1]
1. Wir sagen der Person vorher, was wir mit ihren Daten wozu tun.
2. Wir halten uns daran und setzen Daten nicht zweckwidrig ein.
3. Wir üben uns in Datensparsamkeit und "need-to-know".
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.
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!
Fragen? (FAQ auf https://bit.ly/3RC49c1 und mehr auf https://bit.ly/3RCmuFQ)
Intern:
Extern: (ggf. kostenpflichtig)
[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)
Legende: Umgang mit Daten, Betroffenenrechte, Governance, 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
Alle Rechte vorbehalten. Darf (ausser in den Feldern) unverändert frei weitergegeben/benutzt werden. Dies ist Information, keine Rechtsberatung.
VISCHER


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 (→
Wir prüfen unsere Verträge
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
(falsche oder
mitwirken. Datenschutzrechte 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
eine DSFA. Darin dokumentieren
Vorhaben und die
ativer Folgen für sie
(falls ja: Hilfe holen). Wir bewahren sie auf.
8 Privacy by Default
Wo wir in
datenschutz haben, sind diese auf das Minimum voreingestellt. Die Entwickler achten darauf.
4.2.10. «Kleines Berufsgeheimnis» und die Schweigepflicht
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, Betroffenenrechte, Governance, Prozesse, 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.
VISCHER

4.2.11. Datenschutz-Folgenabschätzung (DSFA)

Datenschutz-Folgenabschätzung (DSFA)

- Strukturierte Prüfung der Risiken einer Bearbeitungstätigkeit für die betroffene Person
- Pflicht, wenn Bearbeitung ein hohes Risiko für die betroffene Person mit sich bringt (Art. 22 revDSG)
  - z.B. bei Installation einer Sicherheitskamera
- DSFA muss mindestens zwei Jahre nach Beendigung der Datenbearbeitung aufbewahrt werden
- Verwendung einer Vorlage sinnvoll, typischer Aufbau:
  - Beschreibung des Vorhabens; Bewertung der Risiken für die betroffene Person; Massnahmen zur Eindämmung der Risiken
- Pflicht für Verantwortlichen (i.d.R. unterstützt durch Provider)



Checkliste Datenschutz (1/2)

Nr.	Aufgabe	Erläuterung	OK	Verantwortung
1	Datenschutzperson Kapitel 4.1	Empfehlung: Benennen Sie jemanden, der sich um den Datenschutz kümmert (kann auch der Inhaber oder die Inhaberin oder jemand aus der Leitung sein)	☐	
2	Bearbeitungsverzeichnis Kapitel 4.2.1	Erstellen Sie ein Bearbeitungsverzeichnis. Ist kein Bearbeitungsverzeichnis notwendig, kann es für die Datenschutzerklärung dennoch sinnvoll sein, sich einen Überblick über die Datenbearbeitungen zu verschaffen und dies (vereinfacht) festzuhalten.	☐	
3	Datenschutzerklärung Kapitel 4.2.2 Muster kibesuisse	Erstellen Sie eine Datenschutzerklärung, die sämtliche Datenbearbeitungen enthält und halten Sie diese aktuell. Ziehen Sie dies, wenn nötig, dem Verzeichnis vor, damit sie möglichst am 01.09.2023 bereitsteht.	☐	
4	Auftragsbearbeiter Kapitel 4.2.5	Prüfen Sie, ob Sie mit allen Auftragsbearbeitern und Auftragsbearbeiterinnen einen Auftragsbearbeitungsvertrag abgeschlossen haben (wo möglich zusammen mit den Auslandtransfers)	☐	
5	Datensicherheit Kapitel 4.2.8	Achten Sie (fortlaufend) auf Ihre Datensicherheit. Fehlt Ihnen das Fachwissen, beauftragen Sie hierzu einen Spezialisten.	☐	

Checkliste Datenschutz (2/2)

6	Auslandtransfers Kapitel 4.2.4	Prüfen Sie Ihre Auslandtransfers und Ihre diesbezüglichen Verträge.	☐	
7	Weisung Kapitel 4.1	Erlassen Sie eine (kurze) Weisung zum Datenschutz, welche den Umgang mit Personendaten festlegt.	☐	
8	Schulung Kapitel 4.1	Schulen Sie Ihre Mitarbeitenden im Umgang mit Personendaten und der Informationssicherheit.	☐	
9	Betroffenenrechte Kapitel 4.2.3	Stellen Sie sicher, dass die Betroffenenrechte eingehalten werden können (z.B. Datenschutzperson)	☐	
10	Umgang mit Personendaten Kapitel 3	Gestalten Sie alle Datenbearbeitungen im Unternehmen den Grundsätzen entsprechend. Achten Sie bei Daten im Rahmen einer öffentlichen Aufgabe auf die Notwendigkeit der Daten für die Aufgabe.	☐	
11	Datenlöschung Kapitel 4.2.7	Stellen Sie sicher, dass Personendaten gelöscht werden können und werden. Empfehlung: In einer Weisung festhalten, wie lange Daten aufbewahrt werden, sowie wann und wie sie zu löschen sind.	☐	

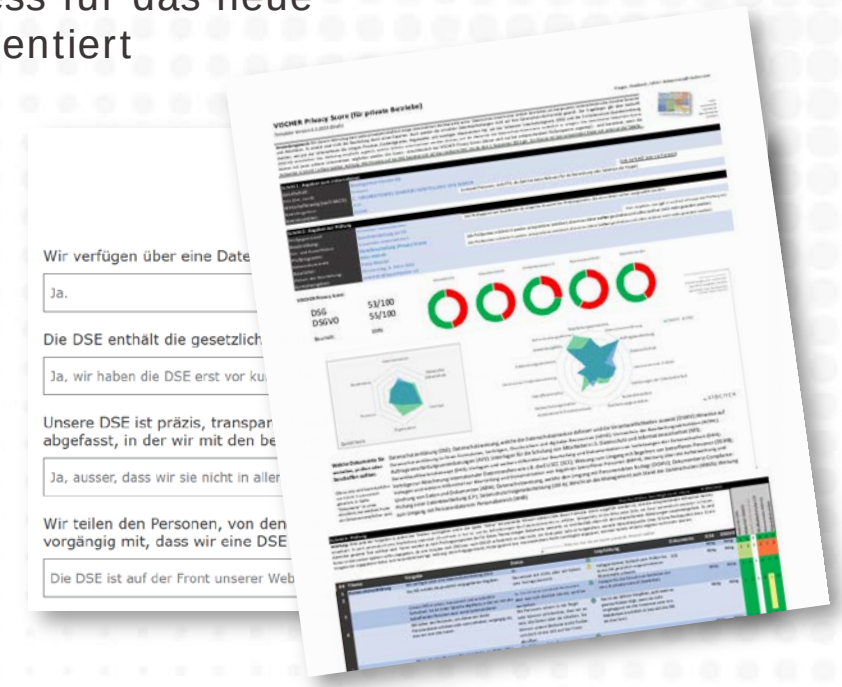
Umsetzungshilfen

- Praxiswegleitung kibesuisse
- Musterdatenschutzerklärung kibesuisse
- Merkblatt für Mitarbeitende kibesuisse
- revDSG - was ist zu tun
- KMU Datenschutzweisung
- Auftragsbearbeitungsvertrag auf einer Seite

Ermitteln Sie Ihren VISCHER Privacy Score

- **Tool** (Online, Excel), welches Ihre Fitness für das neue DSG (und DSGVO) beurteilt und dokumentiert
  - Diverse **Prüfprogramme** (Kurz- und Detail-Prüfung von 25/100 Minuten)
  - Sie erhalten einen **Bericht als PDF**, inklusive Handlungsempfehlungen
  - Auch als **Reporting** für VR und GL
  - Online-Version **kostenlos**, kann ohne Registrierung benutzt werden
  - Jetzt im öffentlichen **Testlauf** – probieren Sie VPS für sich selbst aus:

    privacyscore.ch



Einige häufige Irrtümer

- 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
  - Es galt und gilt: Personendaten müssen gelöscht oder anonymisiert werden, sobald Bearbeitungszweck erfüllt ist und kein berechtigtes Interesse an einer Aufbewahrung besteht
  - eine zu lange Speicherung erhöht zudem die Risiken bei Sicherheitsverletzungen
- Nein, nicht alles, was **DSGVO-"konform"** ist, genügt für das neue DSG (z.B. Datenschutzerklärung, Providerverträge)

Strafrechtliche Sanktionen

- **Strafrechtliche** Sanktionen: Bussen neu bis CHF 250k
  - Bussen für ungenügende DSE und Providerverträge, fehlenden Schutz beim Datenexport in "unsichere" Drittländer, fehlende Datensicherheit, falsche oder unvollständige Auskünfte an Betroffene, Verrat von vertraulichen beruflichen Personendaten
  - Bussen auch für VR und GL, die Verstösse nicht verhindern
  - Wichtig ist daher eine klare Regelung der Verantwortlichkeit

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

Q&A

- Was ist bei der Bearbeitung von Personendaten von Arbeitnehmenden zu beachten?
- Datenlieferung an Unfall/Krankenversicherungen unserer MA? Kommunikation an Pensionskasse?
- Dürfen Lohnabrechnungen noch an die Mitarbeitenden per E-Mail gesendet werden?
- Dürfen Verträge per Mail gesendet werden?
- Dürfen Rechnungen per Mail gesendet werden?
- Wie weit dürfen Anfragen weitergeleitet werden an Tagesfamilien und in welcher Form?
- Verschlüsselungsdienst für E-Mails / SharePoint-Ordner

VISCHER

Vielen Dank für Ihre Aufmerksamkeit!

lhunger@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