

Unsere Datenschutzweisung.

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?

Organisation:

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

<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Wir haben eine separate/weitere Liste

Verantwortliche Person?

Datenbearbeitung Wer?

<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Datenschutzstelle:

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 unbekanntens/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.

Was tun wir mit Daten von Mitarbeitenden?

Wir beschaffen die Daten, die sie uns geben, ferner Daten aus öffentl. 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: GeschäftsführerIn (**GF**), Geschäftsleitung (**GL**), Geschäftsjahr (**GJ**), Ablauf (**AL**), Jahre (**J**)

Eine einfache, allgemeine Datenschutzweisung für KMU.

Testen Sie Ihre DSGVO-Fitness
kostenlos unter privacyscore.ch

Auf der vorstehenden Seite ist eine einfache, aber dennoch alle wesentlichen Punkte abdeckende Datenschutzweisung für kleine und mittlere Betriebe enthalten, die auf das neue Datenschutzgesetz (**DSG**) abgestimmt ist, das ab dem 1. September 2023 gilt.

Sie ergänzt unseren One-Pager "Survival Guide" zum DSG, welcher ebenfalls auf einer Seite alle wesentlichen Vorgaben des DSG enthält. Mit der vorliegenden Weisung kann die Geschäftsleitung einer Organisation diesen One-Pager als Weisung erlassen und zugleich die nötigen Verantwortlichkeiten festlegen. Dem wird unserer Erfahrung nach oft zuwenig Beachtung geschenkt, ist aber speziell vor dem Hintergrund der verschärften Strafbestimmungen zum DSG wichtig (dazu unser Blog <https://www.vischer.com/know-how/blog/wie-straftbarkeit-unter-dem-neuen-datenschutzgesetz-vermieden-wird/>)



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

Um die Weisung zu erlassen, füllen Sie zunächst das erste Weisungsblatt (d.h. die obige Vorlage) in den freien Feldern aus. Geben Sie oben den **Namen der Gesellschaft** an; Sie können oben rechts auch das eigene Logo anbringen.

Als nächstes ergänzen Sie die Tabelle mit den **Aufbewahrungsfristen**. Einige der typischen Aufbewahrungsfristen haben wir schon angegeben, weitere können Sie im Formular oder auf einer separaten Liste ergänzen. Es gilt die Grundregel, dass Sie Unterlagen und Personendaten nur aber immerhin dann vernichten bzw. löschen sollten, wenn sowohl eine etwaige gesetzliche Frist zur Aufbewahrung abgelaufen ist und auch sonst kein Aufbewahrungsbedarf mehr besteht (z.B. weil die Unterlagen noch als Beweismittel benötigt werden könnten, solange die Verjährungsfristen noch laufen). Das ist an sich nicht Teil einer Datenschutzweisung, aber weil das vielerorts fehlt, haben wir es hier gleich in unser Template mit aufgenommen, quasi als "Bonus".

Sie sollten bestimmen, wer für welche Datenbearbeitung **verantwortlich** ist, die **"VP"**. Für jede Aktivität, bei welcher Personendaten bearbeitet werden, muss jemand für die Einhaltung des Datenschutzes verantwortlich sein, d.h. die dafür nötigen Entscheide treffen. Das ist normalerweise der "Business-Owner" der betreffenden Aktivität, weil die Datenbearbeitung für ihn bzw. für sie durchgeführt wird. Er bzw. sie trägt also den Nutzen und die Kosten und

muss daher auch entscheiden. Er bzw. sie wird in der Praxis den an einer Datenbearbeitung beteiligten Mitarbeitenden sagen, was zu tun ist. Wer also beispielsweise die HR-Abteilung leitet, bestimmt, wie lange dort welche Unterlagen aufbewahrt werden, wer Zugang dazu erhält, welche Daten bearbeitet werden, wo sie bearbeitet werden usw. In einem sehr kleinen Betrieb wird das die Geschäftsführung sein.

Diese Person (VP) muss dafür sorgen, dass die Datenschutzvorgaben wie auf dem One-Pager angegeben umgesetzt werden – durch sie selbst, durch Mitarbeitende oder externe Hilfe. Sie muss also dafür sorgen, dass eine Datenschutzerklärung besteht, die "Zehn Gebote" eingehalten werden, die nötigen Verträge mit Dritten abgeschlossen werden, die Datensicherheit gewährleistet ist und die Betroffenenrechte bei Anfragen erfüllt werden. In der Weisung kann die VP für einzelne Datenbearbeitungen aufgeführt werden (z.B. mit dem Kürzel oder "GL").

Eingetragen werden sollte auch, wer die **Datenschutzstelle** ist (soweit es eine solche gibt; bei Kleinbetrieben übernimmt die VP diese Rolle). Sie hat eine koordinierende und beratende Funktion, muss kein(e) Spezialist(in) sein, aber wissen, wo nachzufragen ist und sich um operative Belange kümmern. Ihr Name sollte auch in den freien Feldern auf dem One-Pager mit den Vorgaben eingetragen werden (also unter dem Titel "Wir haben eine Stelle..." und bei "Fragen?" unten rechts).

Schliesslich hat es noch Platz für weitere, **individuelle Hinweise und Weisungen** (z.B. für weitere Dinge, die zu beachten sind oder Unterlagen). Ganz oben links kann eingetragen werden, wer die Weisung wann **erlassen** hat und ab wann sie gilt.

Hinweis: Wir haben als weiteren "Bonus" auch noch eine kleine Datenschutzerklärung für Mitarbeitende eingebaut, dies deshalb, weil eine solche unter dem DSG empfehlenswert ist. Da aber nicht alles Platz hat und wir annehmen, dass alle Unternehmen auch eine "normale" Datenschutzerklärung haben, verweisen wir für die fehlenden Informationen kurzerhand auf einfach diese.

Haben Sie Fragen oder benötigen Sie ausführlichere Templates, Schulungsmaterial oder sonst Hilfe? Schreiben Sie der Person Ihres Vertrauens oder uns auf dataprivacy@vischer.com.