

Datenschutzmerkblatt SVVG

Bei der Erfassung und Verarbeitung personenbezogener Daten müssen alle datenschutzrechtlichen Regelungen – insbesondere das Bundesgesetz über den Datenschutz (DSG) und die Verordnung über den Datenschutz (DSV) – beachten werden. Die Nichtbeachtung kann zu materiellen Schäden, Imageverlust und im Extremfall zu strafrechtlichen Konsequenzen für die einzelne handelnde Person führen. Wir erwarten deshalb einen verantwortungsvollen Umgang mit personenbezogenen Daten. Dieses Merkblatt regelt den Umgang mit Personendaten beim SVVG¹. Es ist **für alle** für den SVVG handelnden und tätigen Personen **verbindlich**.

Was sind Personendaten?

Alle Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen, wie Name, E-Mail, Telefonnummer, Adresse, Geburtsdatum, Kontonummer, Bilder, IP-Adressen, Metadaten über Zugriffe, Nutzungsdauer, Nutzungszeit von Webseiten und Applikationen etc.

Gewisse Daten, wie Daten über die Gesundheit, über religiöse, politische oder gewerkschaftliche Ansichten und Tätigkeiten, über Rasse oder Ethnie, die Intimsphäre gelten als besonders schützenswerte Personendaten. In der Regel werden beim SVVG aufgrund seiner Tätigkeiten keine besonders schützenswerten Daten erhoben.

Zulässige Datenbearbeitungen

Wir Bearbeitung Personendaten immer nach diesen zehn Geboten:

1. Wir beschaffen Daten auf legale Weise und aus rechtmässigen Quellen (Rechtmässigkeit).
2. Wir sagen der Person vorher, was wir mit ihren Daten wozu tun (Transparenz).
3. Wir halten uns daran und setzen Daten nicht zweckwidrig ein (Treu und Glaube / Zweckbindung).
4. Wir sammeln nur die Daten, die wir wirklich brauchen (Datensparsamkeit)
5. Wir löschen rasch, was wir nicht mehr brauchen. (Löschung)
6. Wir tun nur das, was wir bei uns selbst akzeptabel fänden (Verhältnismässigkeit).
7. Wir korrigieren und vervollständigen Daten bei problematischen Fehlern und Lücken. (Richtigkeit).
8. Wir treffen Massnahmen, damit die Daten bei uns sicher sind (Datensicherheit).
9. Wir erlauben einer Person auch "Nein" zu sagen (Widerspruchsrecht).
10. Wir geben sensitive Daten nicht für Zwecke Dritter an Dritte weiter.

Informationspflichten

Wir informieren die betroffenen Personen (Mitglieder, Dienstleister, Kooperationspartner etc.) über die Beschaffung und Bearbeitung von Personendaten in unserer Datenschutzerklärung (DSE). Die DSE wird gut sichtbar und von jeder Seite und Unterseite abrufbar in Deutsch, Französisch und Italienisch auf der Webseite des SVVG publiziert. Sie wird regelässig aktualisiert. Wir weisen auf die DSE hin u.a. in Anmelde- und Mutationsformularen, Verträgen, Newsletter-Disclaimer etc.

Pflichtinhalt: Wer wir sind (mit Kontaktangaben), wozu wir die Daten beschaffen, welche Daten wir bearbeiten, wem wir sie geben (die einzelnen Datenempfänger müssen nicht namentlich genannt werden), in welche Länder oder Regionen sie gehen können und worauf wir uns bei der Datenweitergabe rechtlich stützen.

Datenbearbeitung durch Auftragsbearbeiter

Falls wir Dienstleistern wie z.B. Webseiten-Provider, IT-Dienstleister, Druckereien, Übersetzungsdienste oder sonst jemandem die Bearbeitung unserer Daten anvertrauen, schliessen wir eine Auftragsdatenvereinbarung (ADV) ab, d.h. einen Vertrag, der uns erlaubt, die Datenbearbeitung des Dienstleisters zu steuern und zu kontrollieren und den Beizug von Unterbeauftragten vorab zu genehmigen oder ihm zu widersprechen. Die ADV hält auch die Sicherheitsmassnahmen (sog. technische und organisatorische Massnahmen (TOMs)) fest. Der Auftragsbearbeiter darf nur tun, was wir auch tun dürfen (z.B. i.d.R. keine Datennutzung für sich). Werden Daten mit Dritten wie Dienstleistern, Kooperationspartnern aber auch mit juristisch eigenständigen Regionalverbänden ausgetauscht, prüfen wir, ob eine ADV abgeschlossen werden muss und tun dies wo nötig.

ADV's müssen insbesondere mit Anbietern von cloudbasierten Webdiensten wie z.B. Dropbox, Microsoft OneNote, GoogleDrive, SurveyMonkey etc. abgeschlossen werden. Die Anbieter stellen im Rahmen des Online-Vertragsabschluss-Prozesses regelmässig ADVs zur Verfügung. Wir stellen sicher, dass wir im Namen des SVVG Abos/Lizenzen abschliessen, welche eine ADV beinhaltet. Diese prüfen wir, laden sie runter und bewahren sie zu Beweis Zwecken auf.

Personendaten im Ausland

Problemlos ist die Datenbearbeitung in EWR-Ländern, UK sowie Ländern mit angemessenem Datenschutz gemäss [Anhang 1 der DSV](#). In die USA ist die Datenübermittlung zulässig, wenn das Unternehmen nach dem [Data Privacy Framework](#) zertifiziert ist. In anderen Staaten sowie bei nicht zertifizierte US-Unternehmen ist die Datenweitergabe „nur“ erlaubt, falls:

- Die betroffene Person der Datenbearbeitung im „ungeschützten“ Ausland zugestimmt hat oder
- Standardvertragsklauseln (SSC) mit dem Datenempfänger abgeschlossen wurden und keinen Grund zur Annahme besteht, dass es zu problematischen Datenzugriffen durch Behörden/den Staat kommt.

Datensicherheit

Jeder ist für Sicherheit mitverantwortlich! Wir stellen mit technische und organisatorische Massnahmen (TOMs) sicher, dass die für den SVVG bearbeiteten Personendaten vor unberechtigtem Zugriff durch Dritte geschützt sind.

Technisch: Wir halten uns an das " Need-to -Know“-Prinzip, d.h. nur die Personen erhalten Zugriff auf Daten des SVVG, die diesen für ihre Tätigkeit beim SVVG brauchen. Der Zugang zu Daten erfolgt, wenn immer möglich über persönliche Nutzerkonten. Persönliche Passwörter dürfen nicht geteilt werden. Bei Zugriffsmöglichkeiten von Extern erfolgt eine Mehrfachauthentifizierung. Infrastruktur und Date auf welchen SVVG-Daten bearbeitet werden, sind durch Firewalls, aktualisierte Antimalware-Software und Backups geschützt.

Organisatorisch: Daten des SVVG sind – wenn immer möglich – auf SVVG eigener Infrastruktur und über E-Mail-Adressen des SVVG auszutauschen und aufzubewahren. Wird ausnahmsweise private oder andere Geschäftsinfrastruktur bzw. E-Mail-Accounts verwendet, ist sicherzustellen, dass Daten des SVVG nicht mit anderen geschäfts- oder privaten Daten vermischt werden (z.B. durch Aufbewahrung in einem separaten nur für den SVVG bestimmten Ordner). Die Daten sind sofort zu löschen bzw. sicher zu entsorgen (z.B. durch Schreddern), sobald sie nicht mehr benötigt werden. Für den SVVG tätige Personen, werden regelmässig zu Datenschutz und -sicherheit sensibilisiert.

Zuständige Stelle beim SVVG

Der Geschäftsführer des SVVG ist die SVVG interne Stelle für sämtliche Fragen rund um den Datenschutz. Folgende Themen sind **zwingend** via E-Mail (info@svvg-fsaga.ch, Vermerk Datenschutz) an die Stelle weiterzuleiten:

- **Geltendmachung von Betroffenenrechten:** Gesuche einer Person, die ihre Daten sehen/haben oder diese gelöscht oder korrigiert haben will oder sie sonst ein sie betreffendes Datenschutzanliegen hat.
- **Datensicherheitsverletzungen (Data Breach):** 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 umgehend!
- **Neue Bearbeitungsprozesse:** Wenn wir ein neues oder geändertes Vorhaben haben, das auch Daten von Personen betrifft und daher die Einhaltung des Datenschutzes (ggf. mit Datenschutzfolgenabschätzungⁱⁱ) geprüft werden muss.

Betroffenenrechten

Anfragen von betroffenen Personen werden ausschliesslich in Koordination mit dem Geschäftsführer beantwortet. Die anfragende Person wird vorerst richtig identifiziert. Der SVVG gibt einer Person **Auskunft** über ihre eigenen Personendaten (nicht Dokumente) und auf Wunsch bestimmte weitere Infos. Daten Dritter und eigene Geschäftsgeheimnisse werden dabei geschützt. Die Auskunft erfolgt i.d.R. gratis und innert 30 Tagen. Jede Person kann **Datenkorrektur** verlangen. Ist die Korrektheit 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 berechtigten Grund dafür haben (z.B. Abwicklung der Mitgliedschaft / eines Vertrages).

Meldepflicht bei Verletzung der Datensicherheit (Data Breach)

Ist die Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten verletzt und das Risiko negativer Folgen für einzelne betroffene Personen hoch (nicht bloss lästig) muss der EDÖB über die Datensicherheitsverletzung informiert werden ([Meldeformular](#)). Können sich Personen selbst vor den Folgen schützen, sind auch sie über die Verletzung zu informieren. Data Breaches werden ausschliesslich in Koordination mit dem Geschäftsführer an externe Stellen und Personen kommuniziert. Die Verletzung ist zu dokumentieren und die Dokumentation 2 Jahren aufzubewahren.

Überprüfung und Aktualisierung

Der SVVG kann die Einhaltung des Datenschutzes überprüfen. Verstösse können sanktioniert werden. Das Merkblatt wird in regelmässigen Abständen überprüft und wenn nötig angepasst.

ⁱ Es wird nur auf die für den SVVG relevanten Datenschutzinstrumente und Massnahmen eingegangen. Verzeichnis der Bearbeitungstätigkeiten, Bearbeitungsreglement und Datenschutzberater sind aufgrund der Grösse (< 250 MA) und der vom SVVG vorgenommenen Datenbearbeitungen gesetzlich nicht vorgeschrieben.

ⁱⁱ Eine DSFA ist gesetzlich vorgeschrieben bei heiklen Datenbearbeitungen, u.a. wenn besonders schützenswerter Personendaten in grossem Umfang bearbeitet werden oder neue Technologien (z.B. KI) eingesetzt werden. Eine DSFA ist eine Selbstbeurteilung der geplanten Datenbearbeitung mit folgendem Inhalt: Beschreibung der geplanten Bearbeitung, Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen, Massnahmen zum Schutz der Persönlichkeit und der Grundrechte (Risikominimierung).