

**Programmatisches Dokument zur Datensicherung
des Alpenvereins Südtirol (AVS), mit Sitz in Bozen, Vintlerdurchgang 16,
im Sinne des Datenschutzgesetzes Nr. 196/2003**

Rechtsinhaber der Daten

Dateninhaber der allgemeinen personenbezogenen Daten, die in Ausübung der institutionellen Tätigkeit vom Alpenverein Südtirol (AVS) in dessen Landesgeschäftsstelle in I-39100 Bozen, Vintlerdurchgang 16, bearbeitet werden, ist der Alpenverein Südtirol (AVS), in Person des gesetzlichen Vertreters pro tempore, mit Sitz in I-39100 Bozen, Vintlerdurchgang 16, Tel. 0471/978141, office@alpenverein.it, Webseite www.alpenverein.it, während Dateninhaber der personenbezogenen Daten, die in Ausübung der institutionellen Tätigkeit von den einzelnen Sektionen bearbeitet werden, die jeweilige Sektion ist (siehe unter www.alpenverein.it - Menüpunkt „Sektionen“).

Art der Daten

- a) Im Bereich der Mitgliederverwaltung handelt es sich in der Regel um personenbezogene allgemeine Daten. Die Daten der Mitglieder werden ausschließlich für die institutionellen Zwecke im Interesse der Mitglieder bearbeitet.
- b) Im Bereich der Personalverwaltung und der Buchhaltung werden sensible und allgemeine Daten zu den Mitarbeitern bzw. zu den Lieferanten und Kunden ausschließlich für die vom Gesetz vorgesehenen Obliegenheiten verwaltet.
- c) Kurse: allgemeine und eventuell sensible Daten werden im Interesse des Mitglieds für die beantragten Leistungen erbracht.

Art der Verarbeitung

Erhebung, Sammlung, Registrierung, Verwaltung, Änderung, Archivierung, Löschung bzw. Zusammenstellen und Auswählen von Daten.

Verantwortlicher der Datenverarbeitung, Systemadministrator und Beauftragte

- a) Verantwortlicher für die Datenverwaltung ist der Geschäftsführer Gislar Sulzenbacher
- b) Verantwortlicher Systemadministrator ist der Mitarbeiter Florian Trojer
- c) Beauftragte sind:
 - alle weiteren hauptamtlichen Mitarbeiter sowie evtl. Projektmitarbeiter

- die ehrenamtlichen Mitarbeiter der AVS-Landesleitung und der jeweiligen Referate, sofern sie vom Verantwortlichen für die Datenverwaltung ermächtigt werden
- mit der Überwachung des EDV-Systems und die Ausstellung der Konformitätserklärung gemäß den technischen Vorschriften lt. Art. 25, Anhang B des Datenschutzgesetzes wurde die Fa. ACS Data Systems AG, Brixen beauftragt
- die Wirtschaftsberater Bürogemeinschaft Dr. Vigl & Dr. Friedrich Niedermayr, Bozen
- der Handels- und Dienstleistungsverband Südtirol, Bozen
- Druckereien, die mit dem Versand der Vereinszeitschrift bzw. der Beitragsvorschreibung beauftragt werden
- sowie Bankinstitute und Versicherungen, mit denen der AVS zur Erfüllung seiner institutionellen Ziele zusammenarbeitet.

Risikoanalyse

- a) fehlende oder nicht ausreichende Information der beauftragten Mitarbeiter (geringes Risiko, da die Mitarbeiter ständig informiert werden)
- b) Sicherung der Zugriffsrechte (geringes Risiko aufgrund ausreichender Sicherungsvorkehrungen und ausschließlich individuelle Nutzung der jeweils zugewiesenen PC)
- c) mangelnde Sorgfalt beim Speichern der Daten (geringes Risiko aufgrund ausreichender Sicherungsmaßnahmen)
- d) mangelnde Sorgfalt bei der Ablage der Daten (geringes Risiko, da ausreichende Informationen an die Mitarbeiter, Zugang zum Büro gesichert und Mitarbeiter Kontrollen unterliegen)
- e) Absicherung der EDV-Anlage (geringes Risiko aufgrund ausreichender Sicherungsmaßnahmen)
- f) unbefugter Zugriff und Weitergabe von Daten (geringes Risiko aufgrund ausreichender Sicherungsmaßnahmen)
- g) technische Mängel am IT-System und an Datenträgern (geringes Risiko aufgrund ständiger Kontrollen und ausreichender Sicherungsmaßnahmen sowie ständige Anpassung der IT-Anlage)
- h) menschliches Versagen (geringes Risiko, da wenige Mitarbeiter, umfassende externe Sicherheitskontrolle und ausreichende systematische Absicherung)

Maßnahmen zum Datenschutz

- a) Mitarbeiter bzw. Beauftragte werden geschult und laufend bzw. mindestens einmal jährlich informiert (im direkten Gespräch, Teambesprechungen)
- b) schriftliche Beauftragung und Anweisungen an die beauftragten Mitarbeiter bzw. Einholen deren Zustimmung zur Einhaltung der Maßnahmen
- c) Installation von Authentifizierungssystemen (z.B. Zuweisung und regelmäßige Erneuerung (3 Monate) von Passwörtern (Kombination aus mind. 8 Groß- und Kleinbuchstaben bzw. Zahlen) an den Verantwortlichen und an jeden

Beauftragten bzw. regelmäßiger Austausch dieser); Das Administratorenkennwort wird vom Systemadministrator verwaltet und im Firmtresor aufbewahrt

- d) das Antivirusprogramm und die Firewall werden mit den neuen Updates und Firmware der jeweiligen Hersteller aktualisiert
- e) Datenzugriff haben ausschließlich der Verantwortliche, der Systemadministrator und die Beauftragten
- f) alle Zugriffe auf System und Datenbanken des Systemadministrators werden automatisch registriert
- g) Daten werden täglich gesichert
- h) Geräte (Netzwerk) sind mit Notstromversorgung ausgestattet
- i) alle Softwareprogramme werden laufend bzw. mindestens alle 6 Monate auf ihre Funktionstüchtigkeit kontrolliert und gegebenenfalls aktualisiert. Updates werden laufend eingespielt
- j) Informationen zum Datenschutz an die Mitglieder
- k) es werden nur sichere Datenträger benutzt
- l) Beauftragung einer spezialisierten Firma zur Überwachung des EDV-Systems (inkl. Konformitätserklärung)
- m) jährliche Aktualisierung des Sicherheitsplanes innerhalb 31.03.
- n) schriftliche Zustimmung zur Bearbeitung evtl. sensibler Daten.

Sicherung der Räumlichkeiten

Die Computersysteme und Aktenschränke sind in abgeschlossenen Räumlichkeiten mit kontrolliertem Zugang aufgestellt.

Alle relevanten Daten werden täglich gesichert. Die Sicherungsbänder werden im Serverraum aufbewahrt. Einmal wöchentlich wird eine Datensicherung in ein Bankschließfach gebracht.

Dritte (z.B. Reinigungsfirma, EDV-Firma) erhalten Zugang zu den Räumlichkeiten unter mündlicher Anweisung bzw. unter Aufsicht des Systemadministrators bzw. der anwesenden Beauftragten.

Wiederherstellungsmodalitäten bei Datenverlust

Im Falle von Datenverlusten kann auf die Sicherungsbänder zurückgegriffen werden und mit Hilfe der beauftragten Firma zur Überwachung des EDV-Systems die Wiederherstellung durchgeführt werden.

Schulung der Beauftragten

Die Beauftragten, die mit der Datenverarbeitung betraut sind, werden laufend geschult und über Systemänderungen unterrichtet.

Sie werden bereits bei Eintritt bzw. bei Beauftragung an ihre Pflichten gemäß Dekret Nr. 196/2003 informiert und erteilen ihre schriftliche Zustimmung.

Sie werden angehalten, die Datenverwaltung mit größter Sorgfalt zu betreiben und keine Informationen über die gesammelten und gespeicherten Daten privat zu nutzen bzw. zu verbreiten.

Außerdem sind sie angehalten, die Systeme nur zur Erfüllung der institutionellen Aufgaben zu verwenden.

Diesbezügliche Zuwiderhandlungen ziehen Disziplinarmaßnahmen nach sich.

Sicherungsvorkehrungen bei Auslagerung von Datenverwaltungen an Dritte

Im Falle von Auslagerung an externe Datenverarbeiter werden diese angehalten, alle laut Dekret Nr. 196/2003 vorgeschriebenen Sicherheitsvorkehrungen zu treffen und dies schriftlich zu bestätigen.

Aktualisiert im Februar 2012

Georg Simeoni
Erster Vorsitzender

Gislar Sulzenbacher
Geschäftsführer

Folgende Unterlagen liegen zum Datenschutz vor

- 1) Informationen im Sinne des Art. 13 des Datenschutzgesetzes
- 2) Aufnahmeformular für AVS-Mitglieder
- 3) AVS-Versicherungsschutz - Unfall-/Schadensmeldung
- 4) Ernennung des Verantwortlichen für die Datenverwaltung
- 5) Ernennung des Systemadministrators
- 6) Ernennung des externen Sicherheitsbeauftragten
- 7) Bewilligungssystem und Beauftragte
- 8) Benutzerkonto + Kennwort (Vorlage)
- 9) Konformitätserklärung lt. Art. 25 – technische Vorschriften
- 10) Einwilligung zur Teilnahme an Veranstaltungen und Aktivitäten für minderjährige Teilnehmer (Vorlage)
- 11) Nutzung und Anwendung der Personendaten von AVS-Mitgliedern (Vorlage)