



Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.



VADEMECUM

Privacy e trattamento dei dati personali



Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.



Indice:

- 1. Introduzione**
- 2. Normativa di riferimento**
- 3. Regolamento Europeo 2016/679**
- 4. Definizioni**
- 5. Figure coinvolte**
- 6. Informativa**
- 7. Consenso**
- 8. Esercizio dei diritti dell'interessato**
- 9. Misure di sicurezza**
- 10. Data Breach**



Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.



1. Introduzione

Il presente vademecum è rivolto a tutti i soci del Soccorso Alpino e Speleologico Alto Adige del Corpo Nazionale Soccorso Alpino e Speleologico (C.N.S.A.S.) e può essere considerato un documento riassuntivo ed esplicativo dei concetti fondamentali riguardanti la privacy e il trattamento dei dati personali.

Lo scopo del documento è principalmente pratico; al suo interno sono infatti fornite indicazioni operative al fine di svolgere le attività lavorative quotidiane in armonia con la normativa vigente e nella sicurezza dei dati personali dei soggetti soccorsi e dei soci stessi.

Il vademecum non è da considerarsi un sostituto alla formazione periodica ma anzi un suo supporto, da consultare in caso di incertezza o necessità.

2. Normativa di riferimento

Le norme di riferimento che disciplinano il trattamento e la protezione dei dati sono:

- il **Regolamento Europeo 2016/679** (“*General Data Protection Regulation*”, di seguito anche “*GDPR*”), divenuto applicabile dal 25/05/2018; si tratta della fonte primaria e sovraordinata, direttamente applicabile in tutti i paesi membri dell’Unione Europea, a cui la disciplina nazionale deve allinearsi in base al principio della gerarchia delle fonti del diritto;
- il **d.lgs. 196/2003**, ossia il Codice per la protezione dei dati personali (“*Codice Privacy*”), così come novellato a seguito dell’entrata in vigore del d.lgs. 101/2018, entrato in vigore il 19/09/2018;
- altra normativa nazionale, diversa da quella italiana, di recepimento del Regolamento Europeo.

Ulteriori fonti contenenti disposizioni applicabili al trattamento di dati personali si trovano nei provvedimenti dell’Autorità Garante per la protezione dei dati personali (“*Garante Privacy*”), fra cui rivestono particolare importanza il provvedimento riguardante la figura dell’Amministratore di Sistema (*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*) nonché il provvedimento relativo alla videosorveglianza (*Provvedimento in materia di videosorveglianza - 8 aprile 2010*).

3. Regolamento Europeo 2016/679

La normativa comunitaria introdotta con il Regolamento Europeo 2016/679 (in seguito GDPR) si innesta su un principio cardine e innovativo, ossia il principio di responsabilizzazione (o di **accountability**). Tale principio, vera e propria novità rispetto alla precedente normativa, può essere considerato come il filo rosso che lega e accomuna – sia a livello teorico che a livello pratico – la tutela del dato personale all’interno dell’Unione Europea: al Titolare del trattamento viene richiesto di prendere consapevolezza delle attività di trattamento di dati personali svolte, definendo una



Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.



procedura la quale, fin dalla fase di pianificazione del trattamento (cd principio “**privacy by design**”) e in modo intrinseco a ogni attività effettuata (cd. principio “**privacy by default**”), risulta in armonia con un’idea di fondo che valorizza la protezione e la tutela del dato.

4. Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile anche in modo indiretto. Non sono considerati dati personali i dati riferibili a persone giuridiche, ovvero a imprese, enti e associazioni. I dati personali si dividono in:

- **dati comuni**, ad esempio nome, cognome, codice fiscale, numero di telefono.
- **categorie particolari di dati personali**, i cosiddetti dati “sensibili”: tali dati rivelano l’origine razziale o etnica della persona, le convinzioni religiose e filosofiche, l’appartenenza a organizzazioni sindacali o partiti e opinioni politiche, nonché i dati personali idonei a rivelare lo stato di salute – fisica e/o mentale - e la vita sessuale della persona fisica.
- **dati relativi a condanne penali o reati**, i cosiddetti dati “giudiziari”: tali dati riguardano principalmente il casellario giudiziale di una persona fisica e i carichi pendenti.

I dati non direttamente o indirettamente riconducibili a una persona fisica sono **dati anonimi**.

Per **trattamento di dati personali** si intende qualsiasi operazione o complesso di operazioni applicate a dati personali (ad esempio, si citano le attività di raccolta, la registrazione, la strutturazione, la conservazione, la modifica, la consultazione, l’uso, la cancellazione di dati personali). Le attività di trattamento possono essere effettuate in modalità sia cartacea che elettronica.

5. Figure coinvolte

- **Titolare del trattamento:** soggetto che determina le finalità e i mezzi del trattamento. In senso operativo è rappresentato dal Legale Rappresentante pro tempore.
- **Interessato:** persona fisica a cui si riferiscono i dati personali.
- **Data Protection Officer (DPO):** figura con compiti di consulenza e assistenza al Titolare, nonché di sorveglianza circa l’adempimento degli obblighi posti dalla normativa privacy.
- **Incaricato al trattamento:** soggetto interno all’ente autorizzato al trattamento dei dati da parte del Titolare tramite apposita lettera d’incarico.
- **Responsabile del trattamento:** soggetto esterno all’ente che effettua il trattamento dei dati per conto del Titolare. Viene nominato appositamente e deve prestare garanzie sufficienti a garantire sicurezza e conformità al GDPR.
- **Amministratore di sistema (ADS):** soggetto responsabile della gestione e manutenzione del sistema informatico.
- **Designato privacy:** soggetto di riferimento individuato all’interno dell’ente che ha il compito di comunicare con il DPO e coordinare le attività interne in ambito privacy.
- **Garante privacy:** autorità preposta alla sorveglianza circa la corretta gestione dei Modelli Organizzativi Privacy, nonché all’esaminazione di reclami e segnalazioni. Esegue attività ispettive insieme al Nucleo Speciale della Guardia di Finanza.



Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.

6. Informativa

Ogni socio deve ricevere un'*Informativa sul trattamento dei dati personali* dal Soccorso Alpino e Speleologico Alto Adige. Nell'informativa sono contenute le modalità del trattamento dei dati nell'ambito della gestione del rapporto di lavoro e di adempimento degli obblighi legali. I soci possono sempre avere accesso ai propri dati e richiedere rettifica o cancellazione (ove possibile).

Come i soci, anche tutti i soggetti soccorsi devono ricevere un'informativa al trattamento dati, la quale è presente anche sul sito web del Soccorso Alpino e Speleologico Alto Adige in un'apposita sezione <https://www.soccorsoalpino.org/privacy.html>.

L'informativa può essere consegnata successivamente alla prestazione in caso di emergenza sanitaria secondo l'art. 117 del d.lgs. 31 marzo 1998, n. 112, nonché in caso di impossibilità fisica, incapacità di agire, di intendere o di volere dell'interessato e in caso di rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato.

7. Consenso

Per poter trattare i dati personali in assenza di una delle altre basi previste dalla legge è necessario chiedere il consenso.

Il consenso ha lo scopo di autorizzare o negare l'uso ai dati e deve essere sempre **informato, specifico, libero, consapevole e inequivocabile**.

Nel caso del Soccorso Alpino e Speleologico Alto Adige, il consenso deve essere chiesto ai soci per tutto ciò che non riguarda l'adempimento e la gestione del rapporto di lavoro come ad esempio l'utilizzo di immagini e video sul sito web dell'ente.

Per quanto riguarda i soggetti soccorsi, non è necessario chiedere il consenso per l'utilizzo dei dati sanitari. Basi giuridiche del trattamento sono infatti la salvaguardia degli interessi vitali dell'interessato e l'esecuzione di un compito di interesse pubblico, secondo l'art. 6 lettere d) ed e) del GDPR.

FOTO E VIDEO



Per poter effettuare ed utilizzare foto e video serve **SEMPRE** il consenso! Il Soccorso Alpino e Speleologico Alto Adige dispone di un apposito modulo da consegnare ai soci e da conservare compilato e firmato in un archivio.

MODULO CONSENSI



Il consenso è specifico, cioè riguarda le singole finalità. Nella pratica, questo significa inserire nei moduli una spunta per **OGNI** finalità.

N.B. Nei siti web, **NON** si può inserire una spunta precompilata!



Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.

8. Esercizio dei diritti dell'interessato

L'interessato vanta numerosi diritti nei confronti del Titolare del trattamento che può esercitare in qualsiasi momento.

In particolare, ha sempre diritto di accesso ai dati nonché di modifica, rettifica e cancellazione. Talvolta una cancellazione definitiva è impossibilitata da obblighi di legge (es. per fini fiscali o amministrativi).

L'interessato ha inoltre sempre il diritto di revocare il proprio consenso, anche solo parzialmente, escludendo quindi l'uso dei dati solamente per alcune finalità.

Sul sito web del Soccorso Alpino e Speleologico Alto Adige è presente il *Modulo per l'esercizio dei diritti dell'interessato*.

L'interessato può comunque chiedere con qualsiasi modalità l'accesso, la modifica, rettifica o cancellazione dei propri dati.

È obbligatorio rispondere alle richieste dell'interessato - e quando possibile accontentarle - entro 30 giorni.



9. Misure di sicurezza

Per essere in armonia con il principio di responsabilizzazione e di privacy by design, è necessario mettere in atto misure tecniche e organizzative di sicurezza nella vita lavorativa quotidiana al fine di preservare e gestire in sicurezza tutti i dati personali in possesso dell'ente.

Queste misure si riferiscono alla gestione dell'ufficio, dei documenti, dei profili di autenticazione informatici ma anche a semplici norme comportamentali dei soci.

SICUREZZA IN UFFICIO

Chiudere sempre a chiave l'ufficio in caso di assenza!



Inoltre, è sempre consigliabile chiudere a chiave nei cassetti anche i documenti contenenti informazioni riservate o dati particolari.

Non comunicare mai informazioni riservate o dati particolari durante le telefonate: è impossibile accertare l'identità dell'interlocutore!





Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.



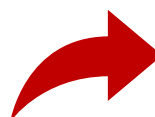
Non comunicare mai a nessuno informazioni su altri colleghi o sui soggetti soccorsi! Tutto ciò che riguarda il lavoro deve restare all'interno dell'ente.

SICUREZZA INFORMATICA



Non utilizzare la posta elettronica dell'ente per ragioni personali!

In caso di assenza impostare un risponditore automatico con avviso e indicazione di un indirizzo alternativo al quale inviare e-mail (altro collega o reparto)



Non comunicare mai a nessuno la password!
È importante che resti privata e venga cambiata ogni 6 mesi.

Attenzione a e-mail ricevute da indirizzi sconosciuti, specialmente se contenenti materiale da scaricare o se richiedono informazioni come credenziali personali: potrebbero essere attacchi informatici.



Ricontrollare sempre i destinatari delle e-mail per non divulgare dati a soggetti non autorizzati e di utilizzare l'opzione CCn (copia conoscenza nascosta) in caso di destinatari multipli.



Soccorso Alpino e Speleologico Alto Adige
Südtiroler Berg- und Höhlenrettung
Aiüt Alpin y Speleologisch de Südtirol
C.N.S.A.S.



10. Data Breach

Con il termine Data Breach si intende qualsiasi “violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati” (art. 4 GDPR). Un Data Breach implica quindi la perdita di almeno una delle caratteristiche di riservatezza, integrità e disponibilità del dato.

Alcuni esempi di Data Breach possono essere un attacco informatico e il furto di un supporto cartaceo e/o informatico.

A seguito di un Data Breach deve essere valutata la gravità della situazione e, quando necessario, notificarlo al Garante della Privacy tramite apposito modulo presente sul sito **entro e non oltre 72 ore**. Nel caso in cui possano esserci rischiose conseguenze anche per gli interessati coinvolti, il data breach dovrà essere tempestivamente comunicato anche a loro con adeguate modalità.

COSA FARE IN CASO DI DATA BREACH?

Contattare **subito** il DPO tramite il proprio superiore.

Sarà il DPO a valutare la gravità della violazione e a consigliare un’eventuale comunicazione al Garante Privacy e/o a tutti gli interessati coinvolti.

Il Soccorso Alpino e Speleologico Alto Adige dispone inoltre di un documento dettagliato chiamato *Procedura Data Breach*, consultabile in ogni momento.

