VADEMECUM

per il trattamento dei dati personali

Versione 2018

Rev.	Data	Motivo
0	26.09.2018	Prima stesura

Data	Approvazione
26.09.2018	Direttivo Associazione

1. INTRODUZIONE E DEFINIZIONI

Il **Vademecum Privacy** è destinato a tutti coloro che, a vario titolo (dipendenti, professionisti, soci, volontari, collaboratori, tirocinanti, ...) sono chiamati a trattare dati personali di utenti o altri soggetti.

Le indicazioni di questo Vademecum sono dirette a evitare comportamenti dai quali possano derivare problemi o pericoli alla sicurezza nel trattamento dei dati, alcuni dei quali sono particolarmente delicati e sensibili e vanno gestiti con riservatezza. Inoltre, vi è da considerare che la gestione dei dati personali è soggetta a precise norme di legge, il cui mancato rispetto può provocare anche conseguenze legali e finanziarie (applicazioni di sanzioni) all'Associazione.

Quindi, con il duplice obiettivo di ottemperare alla normativa e di predisporre un sistema di gestione dei dati che assicuri, soprattutto agli utenti, un trattamento sicuro, è opportuno che le persone che operano all'interno dell'Associazione si conformino ad alcune modalità di comportamento, per la gran parte rispondenti ad un buon senso comune.

Per facilitare l'interpretazione delle indicazioni comportamentali del *Vademecum*, di seguito riportiamo alcune definizioni, tratte dalla normativa.

Definizioni

Dato personale. Qualunque informazione relativa a persona fisica o giuridica, identificata o identificabile, mediante riferimento a qualsiasi altra informazione, ivi compreso il codice di identificazione personale (Codice fiscale o partita IVA).

Dati particolari (o dato sensibile). Sono i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati personali idonei a rivelare lo stato di salute e la vita sessuale, nonché i dati giudiziari.

Archivio (Banca dati). Qualsiasi complesso organizzato di dati personali, in forma cartacea o elettronica, ripartito in una o più unità dislocate in uno o più siti (ad esempio: l'insieme delle cartelle personali degli utenti dell'Associazione è un archivio).

Trattamento. Le operazioni, effettuate manualmente o con l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati personali.

Interessato. La persona fisica o giuridica a cui si riferiscono i dati personali oggetto di trattamento (ad esempio: gli utenti, i soci e i volontari dell'Associazione sono "persone interessate").

Titolare. É l'Associazione A.L.F.I.D., definita come la persona fisica o giuridica, cui competono, anche unitamente a un contitolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Persone autorizzate al trattamento (incaricati). Le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare (Nell'Associazione sono "persone autorizzate al trattamento" tutti coloro che, con diverse finalità, sono chiamate a trattare dati personali di utenti, soci o altri soggetti interessati).

Comunicazione. Dare conoscenza dei dati personali a soggetti determinati (diversi dall'interessato e

dalle persone autorizzate al trattamento), in qualunque forma, anche solo mediante la loro messa a disposizione o consultazione (ad esempio: comunicazione di informazioni relative ad utente ad un Assistente sociale).

Diffusione. Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione (ad esempio: pubblicazione di informazioni "personal" su documenti dell'Associazione o su sito internet).

Dato anonimo. Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile (ad esempio: identificare un utente con un codice o con le sole iniziali rende anonime le informazioni a lui riferite).

2. REGOLE COMPORTAMENTALI NELLA GESTIONE DEI DATI DEGLI UTENTI

Comunicazioni telefoniche e appuntamenti

- Quando si riceve una telefonata di una persona che richiede un primo accesso, fissa un appuntamento o chiede informazioni, i riferimenti e gli appunti vanno riportati nell'agenda di competenza (agenda della segreteria, agenda dei consulenti dipendenti, agenda del terapeuta libero professionista) che va custodita con la massima cura per evitare accessi indesiderati. In particolare, durante l'orario di lavoro è necessario sempre accertarsi che le agende siano sotto il controllo degli operatori e, al termine dell'attività, vanno riposte sempre in cassetto o armadio chiuso a chiave.
- Lo stesso trattamento delle agende va utilizzato per la rubrica generale e la rubrica dei professionisti.
- Le telefonate delle persone che si rivolgono al servizio o che stanno già usufruendo dei servizi dell'Associazione non vanno registrate in nessun caso. Le telefonate pervenute alla segreteria telefonica vanno cancellate dopo l'ascolto.
- Quando vi sia la necessità di inviare notizie di appuntamenti o altre comunicazioni di utenti via e-mail (anche a indirizzi personali) va sempre verificato con attenzione, prima dell'invio, l'indirizzo di destinazione, per evitare di divulgare a terzi non autorizzati informazioni riservate. È buona norma richiedere anche la conferma di lettura (automatica), come ulteriore verifica del destinatario che ha letto la e-mail.

Colloqui con gli utenti

- I colloqui con gli utenti vanno condotti con la dovuta riservatezza, in apposite sale e utilizzando un tono di voce adeguato, in modo che il contenuto del colloquio non possa essere udito all'esterno.
- Al primo colloquio va sottoposta all'utente l'informativa privacy, mettendosi a disposizione per eventuali chiarimenti e raccogliendo sempre il consenso (firma per autorizzazione al trattamento dei dati) sul modulo "Raccolta dati e consenso"

Fascicolo e altra documentazione dell'utente

- I fascicoli degli utenti possono essere consultati solo da persone autorizzate e, una volta utilizzati, vanno riposti nell'apposito schedario chiuso a chiave.

- Evitare di inserire nei fascicoli degli utenti documentazione di carattere sanitario (ad esempio: un certificato medico) o giudiziario (ad esempio: ingiunzione o prescrizione di un giudice), se non strettamente necessario, e comunque solo con l'autorizzazione, anche verbale, dell'utente.
- Quando si predispone o si consulta un fascicolo dell'utente, si deve avere cura di averlo sempre sotto controllo (ad esempio: non allontanarsi lasciandolo incustodito sulla scrivania) e, al termine dell'utilizzo, di riporlo sempre nell'apposito schedario chiuso a chiave.
- I fascicoli degli utenti non devono essere trasferiti all'esterno se non previa autorizzazione del Direttivo e, di norma solo se obbligatorio (ad esempio: ingiunzione di Autorità giudiziaria) o strettamente necessario nell'interesse dell'utente.
- I professionisti esterni che necessitano di portare fuori dai locali dell'Associazione i fascicoli (o documentazione sciolta) dell'utente devono trattarla con la massima riservatezza, adottando accorgimenti analoghi a quelli utilizzati per il trattamento in sede.
- Eventuali dichiarazioni rese su autorizzazione dell'utente (ad esempio: perché richieste da un avvocato da lui nominato, perché richieste dall'Autorità Giudiziaria) devono contenere solo le informazioni essenziali e strettamente richieste dal caso specifico. Evitare in ogni caso di trasmettere documenti forniti dall'utente, se non previa sua esplicita autorizzazione.

3. REGOLE COMPORTAMENTALI NELL'UTILIZZO DI STRUMENTI ELETTRONICI

Sistema gestionale

- L'accesso al sistema deve essere limitato solo alle persone espressamente autorizzate dal Direttivo
- La password di accesso al sistema deve essere cambiata con frequenza almeno trimestrale e comunicata alle persone autorizzate all'accesso con modalità sicure.

Caselle di posta elettronica info@alfid.it, amministrazione@alfid.it, coordinatrice@alfid.it

- Deve essere sempre disponibile l'elenco delle persone autorizzate all'accesso delle caselle di posta elettronica; l'elenco viene gestito da una sola persona a ciò autorizzata (a da un suo delegato sostituto).
- La password di accesso alle caselle di posta va cambiata con regolarità almeno ogni tre mesi e deve essere resa nota alle persone che possono accedere con modalità sicure.
- Quando deve essere esclusa una persona dall'elenco delle persone autorizzate all'accesso (ad esempio: un dipendente che cessa l'attività), la password deve essere cambiata immediatamente (anche se non trascorsi i tre mesi dall'ultima variazione).

Telefoni di servizio dell'Associazione

- I telefoni di servizio vanno utilizzati esclusivamente per le finalità dell'Associazione e protetti da password che va modificata ogni tre mesi.
- Nel caso si sia reso necessario memorizzare indirizzi, numeri di telefono o altri dati anagrafici, questi vanno cancellati dalla memoria del telefono non appena possibile e in ogni caso al termine del servizio reso all'utente.
- In caso di smarrimento o furto del telefono di servizio bloccare immediatamente la SIM.

Telefono privato e personal computer di dipendenti, professionisti, collaboratori e volontari

- Se il dipendente, professionista, collaboratore o volontario utilizzano il telefono privato per i servizi dell'Associazione si richiede di proteggere l'accesso con password (da cambiare almeno ogni tre mesi) e di bloccare la SIM del telefono in caso di smarrimento o furto, avvisando il Direttivo dell'Associazione.
- In caso di utilizzo di personal computer, ad esempio per la stesura di relazioni e verbali riferiti ad utenti, si richiede di proteggere l'accesso con password (da cambiare almeno ogni tre mesi) e, in caso di smarrimento o furto, di avvisare il Direttivo dell'Associazione qualora si ravvisi il rischio che documenti o file relativi agli utenti possano essere memorizzati sul computer personale.
- Le relazioni o altri documenti riferiti agli utenti e predisposti con il proprio computer personale vanno tendenzialmente cancellate dal computer non appena possibile; per il periodo di conservazione è preferibile memorizzare le relazioni su un supporto esterno (quali: pen drive USB, Hard Disk esterno, CD) che va custodito con cura separatamente dal personal computer.

4. ALTRE REGOLE COMPORTAMENTALI DI CARATTERE GENERALE

Indicazioni generali

- Dipendenti, professionisti, collaboratori e volontari devono registrare solo i dati personali degli utenti strettamente necessari, ritenuti utili e attinenti alle finalità del servizio.
- I dati vanno aggiornati ogni qualvolta si venga a conoscenza di eventuali variazioni.
- Come regola generale, è obbligo detenere dati e informazioni dell'utente che non sono inseriti nella cartella utente solo per il tempo strettamente necessario allo svolgimento del servizio.
- Se non strettamente necessario, non è opportuno portare fuori dagli uffici dell'Associazione supporti informatici o cartacei contenenti dati personali.
- Se non strettamente necessario e se l'interlocutore non è conosciuto, si deve evitare di comunicare per telefono informazioni relative a dati particolari e sensibili; in caso di dubbi e necessario accertarsi dell'identità dell'interlocutore (ad esempio: identificare il chiamante e richiamarlo successivamente al numero fornito).
- Custodire con cura le chiavi di schedari, armadi e cassetti, verificando periodicamente che siano ancora presenti e che siano funzionanti (soprattutto per le chiavi che non sono usate frequentemente).

Utilizzo di strumenti informatici

- I computer e gli smartphone (anche personali) non devono essere lasciati incustoditi o accessibili da terzi durante l'utilizzo; in caso di allontanamento dalla postazione di lavoro, spegnere il computer o attivare la funzione di "blocco schermo" (*screen saver).*
- Prima di utilizzare supporti rimovibili (quali: pen drive USB, Hard Disk esterno, CD) di qualsiasi provenienza e buona prassi controllarne il contenuto con un sistema antivirus.
- Per evitare il pericolo di introdurre virus informatici è opportuno porre molta attenzione nelle operazioni di scarico e installazione di programmi software, che vanno effettuate da persone

esperte in grado di riconoscere i siti sicuri da quelli potenzialmente pericolosi.

- Non comunicare le password (del sistema gestionale, della posta elettronica, del computer o dello smartphone) ad altre persone e conservarla con modalità sicure (ad esempio: non scriverla su foglietti esposti sulla tastiera o sul monitor del computer).

Utilizzo della posta elettronica

- Non è buona prassi allegare al testo delle comunicazioni, materiale potenzialmente insicuro o file di dimensioni eccessive (in quest' ultimo caso utilizzare formati compressi come *.zip, *.rar, ecc.)
- Nel caso di mittenti sconosciuti, di messaggi dall'oggetto insolito o comunque in presenza di fondati sospetti sulla pertinenza del messaggio e-mail, per evitare il cosiddetto fenomeno del *pishing* informatico, è consigliata l'eliminazione senza l'apertura del messaggio; lo stesso vale nel caso di messaggi provenienti da mittenti conosciuti che presentano file allegati con particolari estensioni (ad es: *.exe, *.scr, *.pif., *.bat, ...).
- Quando si invia un documento all'esterno, è preferibile utilizzare un formato protetto da scrittura (ad es: *.pdf).
- Qualora il messaggio debba essere inviato a più soggetti terzi, gli indirizzi vanno inseriti solo nel campo "CCn" per tutelare la riservatezza di coloro che ricevono il messaggio conoscendo solamente il mittente e non tutti i destinatari (gli indirizzi possono ovviamente essere tenuti in chiaro se necessario ai fini della comunicazione).
- Prima di iscriversi a *mailing list*, *newsletter* o gruppi di discussione di varia natura è necessario verificare l'affidabilità dell'organizzazione e del sito internet di riferimento.