Documento programmatico sulla sicurezza nel trattamento dei dati personali[1]

Il presente documento è redatto ai sensi dell'art. 34, comma 1, lett. g) del D.Lgs. n. 196/03 (Codice della privacy) e al Disciplinare Tecnico allegato sub B, con lo scopo di descrivere il quadro delle misure minime di sicurezza, organizzative, fisiche e informatiche, da adottare e adottate dall'**Associazione di Volontariato** "……", con sede in ……, via …… n. …, *iscritta al Registro del Volontariato al n. …*, al fine della tutela dei dati personali trattati dall'associazione medesima. L'associazione svolge l'attività di ……[2]

Il presente DPS è redatto e firmato dal Presidente e legale rappresentante dell'Associazione, in seguito indicata anche solo come Titolare.
[oppure]
Il presente DPS è redatto e firmato dal Responsabile del trattamento signor ……[3], ……[4], nominato con lettera del ……[5]

Elenco dei trattamenti di dati personali (19.1. D.T.)

L'associazione svolge i seguenti trattamenti di dati personali[6]:

COD1. trattamento di dati personali comuni[7] e sensibili[8] dei propri soci e/o volontari, relativi alla reperibilità ed alla corrispondenza con gli stessi o comunque necessari, funzionali o connessi alla gestione del rapporto associativo e allo svolgimento dell'attività istituzionale, per le seguenti finalità:

- *creazione, organizzazione, consultazione e utilizzo di una banca dati*
- *invio del giornalino dell'associazione*
- *invio delle convocazioni alle assemblee e altre comunicazioni postali*
- *invio di messaggi di posta elettronica*
- *invio di SMS*
- *……*

COD2. trattamento di dati personali comuni[9] e sensibili[10] dei beneficiari/utenti, relativi alla reperibilità ed alla corrispondenza con gli stessi o comunque necessari, funzionali o connessi all conseguimento delle finalità istituzionali, tra cui:

- *creazione, organizzazione, consultazione e utilizzo di una banca dati*
- *creazione di schede relative a ciascun beneficiario*
- *invio del giornalino dell'associazione*
- *campagna di sensibilizzazione attraverso l'invio di ……*
- *……*

---

[1] Con speciale riferimento al DPS si veda la D/R n. 22. Tuttavia la redazione del DPS presuppone lo studio di tutta la prima parte del libretto (D/R da 1 a 26).
[2] L'indicazione dell'attività sociale è facoltativa.
[3] Nome e cognome.
[4] Qualifica all'interno dell'associazione (es. Presidente, dipendente, volontario…..)
[5] Modello n. IV.
[6] Di seguito sono indicati i principali trattamenti che può svolgere una Odv, la natura dei dati personali e le finalità che i trattamenti possono presentare. Soprattutto le parti in corsivo sono casi ed esempi che possono anche non verificarsi: ovviamente se l'associazione non ha dipendenti o non ha collaboratori o non tratta determinati dati inserirà nel DPS solo le altre ipotesi o le ulteriori qui non delineate. Si consiglia di attribuire a ciascun trattamento un codice (un numero) da richiamare poi nelle altre parti del DPS.
[7] Es. nominativo, residenza, numero telefonico, indirizzo e-mail, numero di cellulare, professione, studi compiuti……
[8] Es. lo stesso nominativo se consente di risalire all'iscrizione all'Associazione, se questa ha carattere religioso, politico, filosofico o sindacale (cfr. D/R n. 11, 12 e 13)
[9] Es. nominativo, residenza, numero telefonico, indirizzo e-mail, numero di cellulare, reperibilità dei parenti o delle strutture che li ospitano……
[10] terapia farmacologica, visite mediche o terapie da fare ……

COD3. trattamento di dati personali di fornitori, collaboratori e professionisti (*commercialisti, avvocati, consulenti del lavoro etc.*), altre organizzazioni non-profit, enti pubblici, o comunque terzi con i quali l'associazione ha periodico contatto, riguardanti la reperibilità e la corrispondenza con gli stessi, nonché richiesti ai fini fiscali o dati di natura bancaria o comunque necessari o funzionali allo svolgimento dell'attività istituzionale;

COD4. *trattamento di dati personali del personale dipendente, necessario alla gestione del rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesto ai fini fiscali o previdenziali o trattamento di dati di natura bancaria per le stesse finalità; trattamento di dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o all'adesione ad organizzazioni sindacali;*

COD5. *trattamento di dati giudiziari dei beneficiari dell'attività sociale, dipendenti o soci e/o volontari, idonei a rivelare i provvedimenti di cui all'art. 3 DPR nr. 313/2002, o idonei a rivelare al qualità di imputato o indagato, forniti dagli stessi o da terzi, necessari o conseguenti allo svolgimento dell'attività istituzionali;*

COD6. *comunicazione dei dati …… ai seguenti soggetti ……, per la finalità di ……*
COD7. *diffusione dei dati ……, mediante ……, per la finalità di ……*

I trattamenti possono comprendere il complesso di operazioni indicate nell'art. 4, comma 1, lett. a) ed in particolare 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 cancellazione e la distruzione dei dati, nei limiti e con le modalità descritte nel presente DPS e nell'informativa rilasciata all'interessato. La comunicazione dei dati avviene nei limiti di legge con riferimento a ciascun tipo di dato.

Strutture dove sono svolti i trattamenti, responsabili delle strutture e distribuzione dei compiti (p. 19.2. D.T.)

I trattamenti COD …… vengono svolti presso la sede dell'associazione, ubicata …… al …… piano di un condominio/in una casa singola/dotata di portone di ingresso con chiusura …… I singoli locali della sede dove si trovano i computer sono dotati ciascuno di porta con chiusura a chiave, così come l'archivio. La sede viene aperta ogni …… da …… e chiusa …… da ……
I trattamenti COD …… vengono svolti presso ……[11]
I trattamenti COD …… vengono svolti anche presso ……[12]
Responsabile della struttura dove vengono svolti i trattamenti COD …… è …… *(es. il dipendente responsabile amministrativo signor …… / il Presidente dell'Associazione……); il trattamento è svolto da lui stesso e da altri soggetti incaricati (es. addetti all'amministrazione/membri del Consiglio Direttivo, volontari…)*

Modalità dei trattamenti

I trattamenti COD …… vengono svolti mediante i seguenti strumenti elettronici[13]:
- ❑ *1 computer con funzioni di server connesso in rete ed a internet, marca ……. modello …… contenente ……, situato presso…… Il sistema operativo del server è …… Nel server è installato il router marca …… modello ……*
- ❑ *1 computer connesso in rete ed a internet, con sistema operativo ……, contenente ……*[14]*, situato presso……*
- ❑ *1 computer non connesso in rete ed a internet, con sistema operativo ……, contenente ……, situato presso……*
- ❑ *1 computer portatile conservato e utilizzato da ……, con sistema operativo ……, contenente ……, situato presso……*
- ❑ *……*

La connessione a internet è di tipo ……

---

[11] *Indicare, se ci sono, le strutture esterne alla sede dove è svolto il trattamento o anche solo la raccolta dei dati.*
[12] *Indicare, se ci sono, le strutture esterne che concorrono a svolgere il trattamento (es. studio del commercialista o del consulente del lavoro: vedi anche la parte del DPS relativa ai trattamenti affidati a soggetti esterni).*
[13] *La descrizione qui sotto è solo esemplificativa. L'associazione può anche ovviamente avere un solo computer non collegato alla rete, o non avere strumenti elettronici. Per le misure di sicurezza da adottare si veda anche la "nota tecnica".*
[14] *Indicare la banca dati esistente nel computer (es. elenco dei soci, elenco dei beneficiari……).*

I trattamenti COD …… sono svolti *anche* mediante archivi e strumenti cartacei.

Analisi dei rischi incombenti sui dati (p. 19.3. D.T.)

Con riferimento alla struttura, i rischi possono consistere in ingressi di estranei a locali/aree, nella sottrazione di strumenti contenenti dati, in eventi distruttivi naturali (es. incendi, allagamenti, condizioni ambientali, ...), o artificiali (es. guasto di sistemi complementari), in errori umani nella gestione della sicurezza fisica.
Tali rischi possono esser definiti medio/bassi, poiché la sede ha una superficie modesta, viene sempre chiusa a chiave, è sempre garantita la presenza di volontari, l'accesso di estranei è controllato costantemente ecc. ……; *inoltre l'impianto elettrico è dotato di dispositivo salvavita. E' stato posto in sede un estintore.*

Con riferimento agli strumenti elettronici, i rischi possono consistere nell'azione di virus informatici o di programmi suscettibili di recare danno, nel malfunzionamento, indisponibilità o degrado degli strumenti, negli accessi esterni non autorizzati, nell'intercettazione di informazioni in rete, nella cancellazione di dati.
I rischi possono essere definiti medi, essendo state adottate le misure di sicurezza minime, che saranno altresì costantemente aggiornate [oppure] *il rischio può essere definito medio/alto, essendo state predisposte, per ragioni e difficoltà tecniche, solo parte delle misure minime di sicurezza, che saranno comunque completate entro il 31.9.2005*[15].
Il rischio di deterioramento e perdita dei dati può essere ritenuto basso, grazie alla conservazione di copie di sicurezza/supporti di memorizzazione in un cassetto chiuso a chiave situato nella stanza …… [oppure] *nell'abitazione del Presidente/Responsabile……*

Con riferimento ai soggetti che trattano i dati, i rischi possono consistere nella sottrazione od uso improprio delle credenziali di autenticazione, nella carenza di consapevolezza, nella disattenzione o incuria, in errori materiali.
A tal fine è prevista la specificazione nelle lettere di incarico dei compiti e degli accorgimenti necessari, opportuni approfondimenti in tema di sicurezza nel corso delle assemblee dei soci e lo svolgimento di corsi periodici almeno annuali…

Misure di sicurezza per il trattamento con strumenti elettronici (p. 19.4. D.T.)

Per ridurre i rischi relativi agli strumenti elettronici verranno adottate entro il …… [oppure] sono state adottate le seguenti misure di sicurezza[16]:

- ciascun incaricato viene dotato dall'amministratore di sistema di un proprio username e di una password di …… caratteri, che va cambiata da ogni incaricato al primo accesso. La password non contiene elementi facilmente ricollegabili all'Odv o all'incaricato. *La nuova password viene memorizzata dall'incaricato e posta dall'incaricato in una busta chiusa consegnata al Responsabile/a …… e da lui custodita in un luogo che garantisca la segretezza*. *Ogni sei mesi ciascun incaricato provvederà a sostituire la propria password e a trasmetterla come sopra* [oppure] *Le password saranno modificate dall'amministratore di sistema e comunicate agli interessati ogni sei mesi.*
- si è disposto che tutti gli incaricati non lascino incustodito o accessibile il computer. *A tale riguardo, per evitare errori e dimenticanze, è stato inserito/verrà inserito lo screensaver automatico dopo …… min. di non utilizzo, con password per la prosecuzione del lavoro*[17].
- Per eliminare e/o limitare il rischio di intrusione e azione di programmi (virus, trojan horse, malware, ecc.), i computer sono dotati di antivirus …… , aggiornato almeno ogni sei mesi / *con funzione di aggiornamento automatico ogni ……*, *ed è stato installato/sarà installato sul server/sui PC che hanno accesso a internet il <u>firewall</u> di marca ……*
- Per ogni singolo computer sarà compiuta, con scadenza semestrale, la funzione di aggiornamento del sistema operativo tramite la ditta ……[18] [oppure] mediante lo strumento windows – update
- E' stato disposto l'obbligo di provvedere alla memorizzazione delle banche dati e dei dati personali contenuti nei computer in dischetti o CD rom (cd. copie di back-up) ogni settimana; incaricato delle operazioni e della custodia dei dischetti è il Responsabile *o l'incaricato* ……
- Con riferimento ai floppy-disk ed in generale ai supporti rimovibili, se contenenti dati sensibili o giudiziari, è stato disposto che siano custoditi in cassetti chiusi a chiave e, se non più utilizzati, siano distrutti o resi inutilizzabili
- Sarà inoltre adottata ogni altra misura che venisse ritenuta utile e necessaria dai tecnici, compatibilmente alle risorse dell'associazione, per migliorare la sicurezza degli strumenti elettronici.

---

[15] L'adozione di tutte le misure minime di sicurezza può essere posticipata entro il 30.9.2005 sono in caso gli strumenti elettronici dell'associazione non consentano l'adeguamento entro il 30.6.2004. cfr. D/R n. 16 e seguenti e "Ricapitolando: gli obblighi e le scadenze in breve".
[16] Cfr. D/R n. 16 e seguenti.
[17] Lo screensaver con password è consigliato ma non obbligatorio.
[18] L'assistenza di una ditta esterna non è obbligatoria ma è una scelta dell'associazione. Cfr. sul punto D/R n. 18 e seguenti.

Misure di sicurezza per i trattamenti non elettronici (p. 27-29 D.T.)

Per ridurre i rischi relativi al trattamento cartaceo e manuale sono state adottate le seguenti misure:

- Si è disposto che gli incaricati non lascino incustoditi sulle scrivanie, o su altri ripiani o in luoghi accessibili all'utenza o al pubblico atti, documenti e fascicoli contenenti dati personali, ma li conservino in appositi schedari/fascicoli, prelevandoli solo per il tempo necessario al trattamento.
- Il locale destinato all'archivio sarà chiuso a chiave. Il dipendente / volontario con funzioni di custode sig. …… / il Responsabile è incaricato di controllare l'accesso all'archivio. Fuori dall'orario di apertura della sede l'accesso all'archivio sarà consentito previa registrazione su un quaderno, qualora l'archivio contenga dati sensibili o giudiziari.

Misure per il ripristino dei dati (p. 19.5. D.T.)

Nell'ipotesi di distruzione o danneggiamento dei dati sensibili o degli strumenti elettronici che li contengono si adotterà la seguente procedura:

- gli incaricati avvertiranno il titolare/*responsabile*[19] e la persona che ha in custodia le copie di back up e i supporti elettronici contenenti i vari software installati nei computer distrutti o danneggiati;
- *il titolare/responsabile chiederà immediatamente l'intervento della ditta addetta alla manutenzione/amministratore di sistema sollecitandone al più presto l'assistenza;*
- il tecnico provvederà a reinstallare i programmi danneggiati o distrutti, o a sostituire il disco fisso o l'intero hardware, reinstallandovi il sistema operativo e i dati e programmi contenuti nelle copie di back-up e provvedendo al loro aggiornamento;
- *verrà richiesto al tecnico della manutenzione di suggerire ogni altra misura;*

In ogni caso, viene data esplicita istruzione che il ripristino dei dati e dei sistemi sia effettuato entro e non oltre 7 giorni dalla distruzione o danneggiamento.

Formazione degli incaricati (p. 19.6. D.T.)

La formazione degli incaricati verrà effettuata all'atto della nomina e dell'assunzione dei compiti relativi, in caso di installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Ogni incaricato riceve inoltre una lettera di incarico contenente i suoi compiti, le istruzioni operative e i limiti del suo trattamento. *Potranno essere indetti specifici corsi di una giornata, destinati a coloro i quali svolgono il trattamento di dati sensibili*. La formazione tende a sensibilizzare gli incaricati sulle tematiche della sicurezza, facendo comprendere i rischi e le responsabilità in cui incorrono (con specificazione delle sanzioni amministrative, penali e disciplinari). Inoltre, essa consiste nella spiegazione del concetto di "dato sensibile", nell'invito a segnalare eventuali disfunzioni dei sistemi operativi e, nel dubbio, di richiedere al titolare *e al Responsabile* ogni chiarificazione o istruzione. La formazione è svolta da ……/dal Responsabile. [20]

Trattamento da parte di soggetti esterni (p. 19.7. D.T.)

Il trattamento n. ……/il trattamento relativo a …… (*es. alla gestione delle paghe e contributi dei dipendenti dell'associazione*) è svolto all'esterno dell'associazione, avvalendosi della collaborazione del dott./rag./…… …… (*es. consulente del lavoro*).
Il trattamento n. ……/il trattamento relativo a …… (*es. alla gestione degli adempimenti fiscali*) è svolto all'esterno dell'associazione, avvalendosi della collaborazione del dott./…… …… (*es. commercialista*).
……

Tali soggetti sono stati nominati Responsabili di quel specifico trattamento[21]. Tali soggetti offrono piena garanzia per il corretto assolvimento del proprio compito, assumono l'obbligo di utilizzare i dati solo per lo scopo a loro assegnato, dichiarano di adottare le misure di sicurezza previste dal Codice e di relazionare periodicamente all'associazione sulle misure di sicurezza adottate.

---

[19] Se nominato.
[20] La formazione degli incaricati è obbligatoria per legge. Se si tratta di soci/aderenti si può risolvere in una spiegazione durante l'assemblea, anche se un breve corso sarebbe l'ideale; se l'O.d.V. ha dipendenti o personale stabile a costoro va fatta probabilmente in modo più accurato. In ogni caso, è essenziale che gli incaricati sappiano utilizzare la loro password e sappiano quali trattamenti possono svolgere e quali sono vietati. Nel fare la formazione ci si può basare sul contenuto del DPS ed eventualmente integrarlo con le più importanti nozioni contenute nella sezione D/R di questo libretto. Si ricorda che, in ogni caso, i compiti (e quindi anche i limiti) per un incaricato devono emergere nella lettera di incarico a lui consegnata (modello IX).
[21] La nomina del soggetto esterno quale Responsabile è facoltativa.

Il presente DPS è conservato presso la sede dell'associazione per essere esibito in caso di controllo; è a disposizione di ogni incaricato e verrà aggiornato entro il ……[22]

……, lì

Il legale rappresentante *Il responsabile*

…… ……

N.B. Cancellare le note a piè di pagina
prima di stampare la versione definitiva

[22] L'aggiornamento del DPS deve essere per lo meno annuale, quindi si potrà scrivere, ad es. 8 aprile 2006 se il DPS è stato redatto l'8 aprile 2005.