

Protocollo Operativo di prevenzione
AVIS Comunale di Legnano e Reati Informatici e trattamento dei dati
Art. 24 bis d.lgs. 231/2001

(approvato dal Consiglio Direttivo dell'AVIS Comunale di Legnano con delibera del 23/02/2016 unitamente all'intero Modello 231 in ottemperanza ai precetti di cui al d.lgs. 231/2001)

INDICE

1. Scopo
2. Applicabilità;
3. Responsabilità;
4. Modalità operative

1. SCOPO

Scopo del presente “Protocollo Operativo di Prevenzione ex art. 24 bis del D.lgs. 231/2001” è quello di individuare le modalità operative e comportamentali che dovranno essere osservate dai soggetti a qualunque titolo coinvolti nell’attività di gestione IT, gestione banche dati e/o gestione dati informatici dell’AVIS Comunale di Legnano nell’assoluto rispetto della legalità e, in particolare, al fine di prevenire situazioni potenzialmente idonee alla commissione di fattispecie criminose ritenute rilevanti ex d.lgs. 231/2001, quali in particolare quelle di cui all'art. 24 bis del medesimo decreto, salvo la commissione delle medesime in maniera del tutto fraudolenta.

Gli Organi sociali e i dirigenti, nonché i lavoratori dipendenti, i consulenti e i liberi professionisti dell’AVIS Comunale di Legnano – ovvero tutte le funzioni a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo dei sistemi informatici e del patrimonio informativo dell’azienda- , sono peraltro tenuti ad osservare i seguenti **principi generali**:

- L’utilizzo degli strumenti e dei servizi informatici e/o telematici dell’AVIS Comunale di Legnano deve avvenire nel pieno rispetto delle normative vigenti in materia di illeciti informatici, sicurezza informatica e di disciplina del trattamento dei dati personali nonché nel rispetto delle procedure interne di sicurezza aziendale in materia di utilizzo e gestione degli strumenti stessi (Procedura Generale Gestione informatica; Organigramma e responsabilità; Registro dei trattamenti e DPIA ai sensi del Regolamento Europeo n.679/2016.
- Consentire l’accesso e utilizzo dei medesimi strumenti ai soli soggetti autorizzati;
- Gli organi sociali e il Direttore Generale, di concerto con l’OdV e con il responsabile dei Sistemi informatici, devono organizzare un sistema di comunicazione, informazione e formazione del personale in materia di utilizzo dei sistemi informatici e telematici e degli asset informatici telematici aziendali, con particolare riferimento ai rischi connessi allo svolgimento dell’attività ed alle misure di sicurezza prescritte dall’AVIS Comunale di Legnano (tale sistema deve riguardare i soggetti destinatari di particolari compiti in materia informatica);
- I rapporti instaurati dall’AVIS Comunale di Legnano con collaboratori e/o fornitori di servizi informatici devono essere contrattualizzati per iscritto e contenenti la clausola che imponga loro , nello svolgimento delle loro attività, il divieto di comportarsi in violazione del d.lgs. 231/2001 in alternativa alla predisposizione della predetta clausola, a detti fornitori o collaboratori potrà esser sottoposta “per presa visione ed accettazione” un’apposita ed unica dichiarazione scritta con cui i

medesimi si impegnano (fino alla cessazione del rapporto con AVIS di Legnano e con riferimento alle attività svolte per essa) al rispetto del presente Modello adottato dall'AVIS di Legnano.

Pertanto ai summenzionati soggetti, in via preventiva alla commissione dei reati in oggetto, è severamente **vietato**:

- accedere abusivamente (intendendosi per accesso abusivo quell'accesso in sistemi informativi e banche dati altrui nella assoluta assenza di autorizzazioni all'accesso ad un sistema protetto) ad un sistema informatico o telematico di associazioni o di terze parti anche con finalità che possano direttamente o indirettamente produrre vantaggio o interesse per l'AVIS di Legnano (es. reperendo informazioni e dati);
- ricevere, detenere o diffondere abusivamente (la detenzione abusiva o la diffusione si caratterizzano dall'assenza di legittimazione alla detenzione o diffusione dei codici) e in qualsiasi forma, codici di accesso per accedere a sistemi informativi o telematici di altre associazioni, altri donatori o di terze parti, anche qualora tale comportamento possa direttamente o indirettamente produrre un vantaggio o un interesse per la associazione (es. utilizzando tali codici per accedere al sistema altrui e compiere operazioni illecite);
- l'eventuale produzione di un documento informatico eseguita fruendo dei servizi di operatori qualificati e certificabili, attraverso chiavi di crittografia legittimamente possedute, verificando che il contenuto del documento sia corretto e veritiero e rendendo all'operatore dichiarazioni o attestazioni vere;
- di procurarsi, diffondere apparecchiature, dispositivi o programmi informatici, attraverso strumenti aziendali, personali o di terze parti, diretti a danneggiare o interrompere un sistema informatico o telematico anche con finalità che possano direttamente o indirettamente produrre un vantaggio o un interesse per l'ente;
- le pratiche di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, e di semplice installazione di strumenti che possano conseguire tali scopi, anche con finalità che possano direttamente o indirettamente produrre un vantaggio o un interesse per l'associazione;
- di eseguire azioni od operazioni che possano causare il danneggiamento di informazioni, dati e programmi informatici di terze parti, in particolare se utilizzati dallo Stato o da altri ente pubblico o comunque di pubblica utilità.
- diffondere all'esterno dell'azienda codici di accesso ai sistemi informatici interni,
- utilizzare password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione;
- lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (familiari, amici)

3. APPLICABILITA'(destinatari)

Il presente Protocollo si applica ogniqualvolta, l'AVIS Comunale di Legnano – per mezzo dei proprio organi apicali, dipendenti o collaboratori esterni – dovesse gestire e/o utilizzare sistemi e dati informatici.

In particolare, detta procedura avrà luogo ogniqualvolta l'AVIS agisca nelle c.d. “aree sensibili di rischio” di cui alla Sez. II di Parte Speciale, quali nella specie:

- ✓ La Gestione di accessi, account e profili: gestione dei servizi IT (trattamento di banche dati e/o dati informatici; tenuta dei registri);
- ✓ La Gestione dei sistemi hardware e software;

- ✓ La Gestione dell' accesso ed utilizzo Sistema Software EmoNet (da parte dei dipendenti AVIS Comunale di Legnano).

3. RESPONSABILITA'

Il presente protocollo trova applicazione nei confronti di tutti i destinatari del Modello medesimo e di tutti coloro che sono coinvolti, a qualsiasi titolo, nella gestione e utilizzo dei sistemi gestione informatica AVIS Comunale di Legnano.

In particolare, conformemente a quanto riportato della "Procedura generale gestione informatica" (PG 7.3) – quale procedura integrante il Protocollo in questione - si applica a:

- *Direttore Generale*: in quanto responsabile di tutto l'applicativo informatico (che, in ragione della propria funzione è peraltro tenuto ad esperire un controllo sul personale ed a valutarne la competenza);

- *R.A.A.*: tenuto alla gestione dell' organizzazione e verifica delle attività amministrative in forza delle indicazioni del D.G., nonché ad assicurare e verificare le attività necessarie per un corretto funzionamento delle apparecchiature informatiche (pc, stampanti e data-base Avis), dei servizi web (sito internet, newsletter e data-base mail donatori) e del backup (sicurezza dati informatici) ed è altresì responsabile dell'inserimento numerico nel data base dell'AVIS Comunale di Legnano in merito alla pianificazione e programmazione delle donazioni e degli esami di controllo;

- *amministrativi e gli infermieri* che – in ragione delle loro mansioni – procedono al salvataggio dei dati informatici relativi al donatore;

nonché a:

- tutte le funzioni coinvolte nella gestione e utilizzo dei sistemi informatici (utilizzanti software della P.A.);

- tutte le funzioni deputate alla progettazione , realizzazione o gestione di strumenti informatici, tecnologici; o di telecomunicazione;

- tutte le funzioni che hanno la responsabilità di realizzare interventi di tipo organizzativo, normativo e tecnologico per garantire la protezione del patrimonio informativo nelle attività connesse con il proprio mandato e nelle relazioni con terzi che accedono al patrimonio informatico;

- tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, forma, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzi i sistemi informativi e trattano i dati del patrimonio informativo.

5.MODALITA' OPERATIVE

Ai fini della prevenzione di detti "reati presupposto" contemplati nella presente Sezione II di Parte Speciale, i destinatari del modello conformano la loro attività alle procedure aziendali adottate, quale nella specie (come già ampiamente anticipato nella Sez.II della Parte Speciale):

- La *Procedura Generale di Gestione informatica* (PG 7.3)(autorizzazione accessi informatici; gestione antivirus; gestione back up; gestione archivi e personale incaricato)

L'AVIS Comunale di Legnano ha, in effetti, predisposto tale presidio organizzativo al fine di prevenire e controllare i rischi in materia di tecnologia dell'informazione, a tutela del proprio patrimonio informatico, nonché la riservatezza dei dati personali e la sicurezza dei sistemi informatici aziendali rispetto ai rischi di distruzione o perdita delle informazioni, accesso non autorizzato e trattamento non consentito.

Peraltro, fermo restando quanto già espressamente previsto dalla summenzionata Procedura, l'AVIS Comunale di Legnano – in forza dei ruoli e responsabilità di cui al par. 3 – assicura che le risorse umane impegnate nell'area IT siano idonee al ruolo ricoperto e consapevoli delle proprie attività (al fine di ridurre rischi derivanti da azioni che ledano l'integrità, riservatezza e fruibilità del patrimonio informativo ovvero da usi non autorizzati del medesimo patrimonio) per mezzo di verifica delle competenze professionali e per mezzo della predisposizione di attività formative in favore dei medesimi.

In particolare:

- quanto alla **gestione degli accessi, account e profili**, l'AVIS Comunale di Legnano garantisce adeguati livelli autorizzativi, quali:
 - definisce formalmente i c.d. “profili di accesso” in ragione dei ruoli e delle funzioni svolte per o presso l'AVIS Comunale di Legnano e i requisiti di autenticazione ai sistemi informatici/telematici per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
 - assegna dunque codici identificativi (user- id) per l'accesso alle applicazioni ed alla rete siano individuali ed univoci (ogni utente è associato ad un unico profilo abilitativo);
 - definisce la corretta gestione delle password attraverso linee guida - comunicate a tutti gli utenti - per la selezione e l'utilizzo della parola chiave; definiti altresì i criteri e le modalità per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (es. lunghezza minima della password, regole di complessità, scadenza);
 - definisce i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente (le variazioni al contenuto dei profili di accesso devono essere eseguite dalle funzioni deputate al presidio della sicurezza informatica, su richiesta delle funzioni interessate e previa verifica in ordine alla corrispondenza delle abilitazioni informatiche);
- quanto alle operazioni riguardanti la **gestione dei sistemi hardware e software**, che comprende anche la gestione del back up e della continuità dei sistemi informativi e dei processi ritenuti critici, l'AVIS Comunale di Legnano:
 - individua i criteri e le modalità per la gestione dei sistemi hardware, prevedendo la compilazione e la manutenzione di un inventario aggiornato dell'hardware in uso presso l'ente e regola le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware;
 - definisce i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società, l'utilizzo formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi;
 - definisce i criteri e le modalità per l'attività di back up che prevedano, per ogni applicazione hardware, la frequenza dell'attività, le modalità, il numero di copie ed il periodo di conservazione dei dati.

Infine, chiunque - nello svolgere la propria funzione - accerti, venga a conoscenza o nutra fondati sospetti circa:

- a) La commissione di fatti od atti rilevanti ai fini della integrazione delle fattispecie di reato di cui alla presente Parte Speciale;
- b) La violazione dei principi e dei protocolli di condotta contemplati nella presente Parte Speciale (o nella documentazione costituente parte integrante della medesima);

è tenuto a darne immediata comunicazione all'OdV, il quale si attiva per l'adozione dei provvedimenti opportuni, nel rispetto di quanto previsto dalla "Procedura di denuncia e segnalazione all'OdV" allegata al presente Modello .

Lo stesso OdV, nell'ambito delle proprie funzioni di controllo, è tenuto – anche con il supporto delle altre figure competenti – a:

- Curare, o fare in modo che sia curata, l'emanazione e l'aggiornamento di istruzioni standardizzate, relative all'uso degli strumenti informatici e alla riservatezza nel trattamento dei dati;
- Verificare periodicamente il sistema di deleghe e distribuzione dei compiti e responsabilità in materia informatica, raccomandando le opportune verifiche;
- Verificare periodicamente la previsione e validità di eventuali clausole contrattuali standard esistenti ,
- Condurre ispezioni e verifiche – periodiche ed a campione – o in occasione di significativi cambiamenti della struttura e dell'organizzazione aziendale;
- Esaminare le eventuali segnalazioni ricevute in ordine ai sistemi informatici ed effettuare gli opportuni accertamenti;
- Indicare agli organi e alle funzioni competenti eventuali proposte di miglioramento.

In casi di particolare urgenza nella formazione o nell'attuazione della decisione o in caso di impossibilità temporanea, sono ammesse eventuali deroghe al rispetto delle prescrizioni contenute nella presente sezione, purché di tale deroga sia data immediata comunicazione all'OdV.