DOCUMENTO

Doc.VPD

VADEMECUM PER LA PROTEZIONE DEI DATI

REVISIONI DOCUMENTO		DESCRIZIONE DELLE MODIFICHE ALLA VERSIONE PRECEDENTE
REV. N°	DATA	
0	12/04/2018	Prima Emissione

INDICE

PREMESSA

Il **Regolamento Generale sulla Protezione dei Dati Personali n. 2016/679** (General Data Protection Regulation o **GDPR**) è la normativa di riforma della legislazione europea in materia di protezione dei dati.

Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, il Regolamento Europeo, entrato in vigore il 24 maggio 2016, ha fissato il termine ultimo per adeguarsi ai nuovi obblighi in materia di protezione dei dati personali al **25 maggio 2018**.

Il **Regolamento UE 2016/679** sancisce il diritto alla protezione dei dati personali, prerogativa fondamentale della persona, e garantisce che il trattamento di queste informazioni "*si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale*".

Il **Regolamento UE 2016/679** dà, inoltre, puntuali indicazioni sul profilo e sulla responsabilità di tutti i soggetti coinvolti nel trattamento di dati personali e stabilisce nuove e pesanti sanzioni, in caso di violazione.

Poiché **l'Avis– Associazioni Volontari Italiani Sangue**, svolgendo la propria attività e perseguendo la mission associativa, deve trattare i dati personali dei propri soci e, per gestire le idoneità dei propri donatori, può venire a conoscenza di categorie particolari di dati (ex dati sensibili), soggiace al regolamento europeo in materia di protezione dei dati personali.

Il presente vademecum si rivolge, dunque, a tutte le **Avis** con l'obiettivo di indicare le novità più rilevanti e fornire indicazioni sugli adempimenti necessari ai fini dell'applicazione del **Regolamento europeo**.

Di seguito vengono specificati i soggetti (profili professionali) coinvolti ed i relativi adempimenti, in parte formali ed in parte sostanziali, che possono variare da associazione ad associazione.

1. SCOPO

Scopo del presente "Vademecum" è quello di indicare le novità più significative e fornire idonee istruzioni per gli adempimenti necessari all'applicazione delle prescrizioni del **Regolamento UE 679 del 2016**, secondo quanto previsto dall'art. 29, secondo cui: "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

Le informazioni contenute nel documento e gli allegati hanno valore indicativo, limitandosi a tracciare le regole basilari comuni previste nel Regolamento europeo e pertanto devono essere approfonditi e adattati alle specifiche esigenze della struttura associativa.

2. CAMPO DI APPLICAZIONE

Il documento si applica, in generale, al **trattamento di dati personali di persone fisiche**, definite "Interessati" (nella fattispecie: soci sia donatori che non donatori e tutti coloro che, a vario titolo hanno rapporti con l'Associazione stessa), contenuti in un archivio ed effettuato per i compiti istituzionalmente previsti con o senza l'ausilio di strumenti informatici.

Ogni Associazione, infatti, nella gestione quotidiana tratta dati personali, ossia raccoglie, consulta, conserva ed in generale gestisce informazioni (elenchi dei soci, dei quali di norma conoscono, oltre alle generalità anagrafiche ed ai recapiti, il gruppo sanguigno, il numero delle donazioni effettuate e la loro data, il giudizio di idoneità o meno alla donazione) per mezzo di strumenti elettronici o mediante documentazione cartacea.

3. DEFINIZIONI E ABBREVIAZIONI UTILIZZATE

È stato predisposto un elenco delle definizioni e dei significati dei termini maggiormente utilizzati per la redazione del presente documento, apportando alcune integrazioni a quelle riprese dall'art. 4 del **Regolamento**:

Amministratore di sistema	Soggetto cui è conferito il compito di sovrintendere alle risorse di una rete o di un sistema base e di consentirne l'utilizzazione.
Archivio	*Insieme strutturato di dati accessibili secondo i criteri determinati*
Autorità di controllo	*l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento.*
Banca dati	Qualsiasi insieme di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati, tali da facilitarne il trattamento.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Dati identificativi	i dati personali che permettono l'identificazione diretta dell'interessato.
Dati biometrici	i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati genetici	*i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.*
Dato personale	*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.*
Dato personale particolare (ex dati sensibili)	i dati personali che rivelino *l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi ad indentificare in modo univoco una persona fisica, i dati relativi alla salute, alla vita o all'orientamento sessuale.*
Dati relativi alla salute	*i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.*
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Persone autorizzate al trattamento (ex Incaricati)	*le persone che sono state autorizzate dal Titolare o dal Responsabile a trattare dati personali secondo le istruzioni documentate fornite dal Titolare, impegnate (o obbligate) alla riservatezza.*
Interessato	*è la persona fisica cui si riferiscono i dati personali.*
Profilazione	*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.*
Pseudonimizzazione	*Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.*
Responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Sistema di autenticazione	è un dispositivo atto a stabilire e verificare in modo univoco, anche indiretto, l'identità dichiarata da un utente che vuole accedere al sistema, prima di ulteriori interazioni tra il sistema e l'utente.

4. RESPONSABILITÀ

Si riporta di seguito la matrice di attività/responsabilità per una immediata individuazione delle varie responsabilità nelle fasi di applicazione e controllo della procedura.

	Rappresentante Legale	Responsabili del trattamento dati	Incaricati del trattamento dati (interni)	Incaricati del trattamento dati (esterni)	Amministratore di sistema	RPD (DPO)	Consulente informatico
Nomina dei responsabili trattamento	**R**					**C**	
Nomina incaricati trattamento dati	**R**	**R**				**C**	
Comunicazione avvio o Modifica trattamento dati		**R**				**I**	
Predisposizione relazione su misure di sicurezza per trattamenti dati		**R**				**I**	
Predisposizione relazione su misure di sicurezza informatiche e adozione adempimenti tecnici in materia						**I**	**R**
Trattamento dati		**R**	**R**	**R**	**R**	**I**	**R**
Redazione del Registro del Trattamento			**C**			**R**	**C**
Censimento trattamento dati			**C**			**R**	**I**
Comunicazioni e notificazioni al Garante Privacy		**R**				**C**	
Consulenza in materia di privacy						**R**	R per quanto riguarda i trattamenti informatici

Legenda Livello di responsabilità		
R = Responsabilità primaria (responsabilità primaria sulla attività nel suo complesso)	**CR = Corresponsabilità** (responsabilità vincolante su una parte della attività)	**CO = Collaborazione** (contribuzione allo svolgimento dell'attività)

5. I SOGGETTI DELLA DATA PROTECTION

Il trattamento dei dati personali, in conformità a quanto previsto dal **Regolamento**, è ammesso solo da parte dei soggetti di seguito indicati:

- Titolare del trattamento;
- Contitolare del trattamento
- Responsabili del trattamento de i dati;
- Persone autorizzate al trattamento (ex Incaricati)
- Data Protection Officer (DPO).

L'Associazione non deve consentire il trattamento dei dati da parte di personale non autorizzato.

5.1 Il TITOLARE DEL TRATTAMENTO

Titolare del trattamento (*data controller*) è la persona fisica, la persona giuridica, che determina le finalità e i mezzi del trattamento dei dati personali in sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.

Il **Titolare** del trattamento dati, nella fattispecie, è ogni singola struttura associativa **Avis**.

In applicazione del principio di *accountability*, il Titolare è responsabile delle attività di trattamento e, con il supporto del Responsabile della Protezione dei Dati (RPD) o Data Protection Officer (DPO), se nominato, in particolare deve:

a) **incaricare** i Responsabili del trattamento dando le necessarie istruzioni per la corretta gestione e tutela dei dati personali;
b) **garantire l'adempimento** agli obblighi previsti dalla normativa in materia di protezione dei dati personali;
c) garantire che le attività di trattamento **rispettino i principi** generali del regolamento;
d) predisporre **misure adeguate** ed efficaci per garantire la sicurezza dei dati.

È necessario che **Avis**, in quanto Titolare del trattamento e nello svolgimento delle proprie attività, sia consapevole sul proprio ruolo nel tutelare il diritto fondamentale alla riservatezza degli interessati (*data subjects*), ma anche quali sono le sanzioni, attualmente inasprite dal Regolamento, per effettuare una **valutazione del rischio** del trattamento per i diritti e le libertà delle persone fisiche e una gestione adeguata della protezione dei dati.

5.2 Il CONTITOLARE DEL TRATTAMENTO

Nello svolgimento dei propri compiti istituzionali, **Avis** può avere necessità di collaborare con terzi, pubblici o privati. Tali ipotesi prevedono una diversa disciplina, con riferimento al trattamento dei dati personali, a seconda che il terzo assuma il ruolo di collaboratore esterno, coadiuvando l'Associazione in un'attività che ricade interamente nella sfera di titolarità e responsabilità di quest'ultima, che conserva pertanto la qualità di unico titolare del trattamento, oppure può rivestire un ruolo del tutto distinto rispetto ad essa, decidendo autonomamente in ordine alle finalità e modalità del trattamento dei dati personali ed assumendone le relative responsabilità.

Nel primo caso **Avis** è titolare esclusivo del trattamento e ha la facoltà di designare il terzo quale "Responsabile esterno del trattamento".

Nel secondo caso invece **Avis** e il terzo si configurano quali autonomi titolari o **contitolari** del trattamento.

5.3 RESPONSABILE DEL TRATTAMENTO

Il Titolare, nella persona del suo legale rappresentante, può **nominare** un **Responsabile del trattamento**.

Il **Responsabile del trattamento** è la persona fisica o giuridica che tratta dati personali, per conto del titolare del trattamento.

Il **Responsabile del trattamento** è tale se ha ricevuto uno specifico incarico, disciplinato da un contratto od altro atto giuridico come disciplinato dall'art. 28 del Regolamento.

Il responsabile ha il dovere di agire secondo le istruzioni fornite dal titolare e di impartirle in senso conforme ai suoi dipendenti e collaboratori che accedono ai dati che ha fornito il titolare.

5.3.1 LA NOMINA DEL RESPONSABILE DEL TRATTAMENTO

I Responsabili del trattamento dei dati vengono designati dal Titolare, ossia **Avis**, nella persona del suo legale rappresentante (il Presidente).

Come previsto dall'art. 28 comma 1 del Regolamento, i Responsabili del trattamento dei dati sono individuati tra soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

Nella fattispecie, per le **Avis** che gestiscono una UdR (Unità di Raccolta di sangue), l'incarico di Responsabile del trattamento dei dati coincide con la titolarità di un incarico di Responsabile di Unità di Raccolta.

L'incarico di **Responsabile di Unità di Raccolta** associativa comporta, in linea generale, l'attribuzione di responsabilità del trattamento dati esclusivamente con riferimento al coordinamento delle attività di raccolta della UdR e delle articolazioni organizzative afferenti (e non quindi la responsabilità di tutti i trattamenti dati ascritti a ciascuna delle articolazioni che fanno parte dell'UdR stessa).

L'incarico di Responsabile del trattamento dati, essendo legato all'incarico di **Responsabile di Unità di Raccolta**, decade automaticamente con la cessazione di quest'ultimo.

L'incarico di Responsabile del trattamento dei dati può essere affidato anche previa valutazione, da parte del Titolare, delle peculiarità dei singoli casi concreti: per esempio soggetti esterni che, per svolgere la propria attività sulla base di convenzione/contratto con l'associazione, vengono in contatto con dati di cui è titolare **Avis** (Responsabili esterni).

La **nomina** è effettuata con apposito atto di nomina redatto secondo il modello facsimile **(allegato A)** che deve essere sottoscritto per accettazione dal Responsabile del trattamento (o Responsabile dell'Unità di Raccolta associativa interessata), in occasione del conferimento dell'incarico e/o unitamente alla sottoscrizione del contratto o altro atto giuridico con il quale lo stesso e affidato.

5.3.2 LE FUNZIONI DEL RESPONSABILE DEL TRATTAMENTO

Il Responsabile del trattamento dei dati è colui che gestisce, per conto di **Avis**, i trattamenti correlati alle funzioni attribuite. Il Responsabile deve:

- attenersi alle istruzioni impartite dal Titolare nell'atto di nomina,
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza,
- adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente.

Il Responsabile deve in particolare assicurare che i trattamenti dati gestiti:

- siano connessi con l'esercizio delle funzioni istituzionali e che le stesse finalità non siano perseguibili attraverso il trattamento di dati anonimi (principio di **pertinenza** e principio di **necessità**);

- che le modalità del trattamento garantiscano il diritto alla riservatezza dei terzi (principio di **non eccedenza**);
- non siano difformi dalle norme di legge e di regolamento.

Ogni Responsabile del trattamento di dati personali deve verificare periodicamente la sussistenza dei requisiti di cui al punto precedente con riferimento alle diverse fasi del trattamento, anche nei casi in cui l'interessato abbia fornito all'organizzazione di sua iniziativa i propri dati personali.

È altresì compito del Responsabile assicurarsi che il trattamento dei dati "sensibili" dell'interessato finalizzato all'erogazione della prestazione sia preceduto dalla preventiva acquisizione del consenso.

Il Responsabile collabora con il **DPO** (se nominato) provvedendo:

a) a fornire ogni informazione dallo stesso richiesta;
b) a comunicargli tempestivamente ogni notizia rilevante ai fini della tutela della riservatezza;
c) a comunicargli tempestivamente l'inizio di ogni nuovo trattamento dei dati nonché la cessazione o la modifica dei trattamenti già in essere;
d) a trasmettere annualmente al medesimo la relazione sulle misure di sicurezza.

Il Responsabile deve assicurare che tutti i soggetti autorizzati al trattamento (dipendenti, lavoratori parasubordinati, soggetti con incarico libero professionale, lavoratori autonomi occasionali, soggetti ammessi allo svolgimento del tirocinio o della frequenza volontaria o che fruiscono di istituti similari), che, nell'ambito dei trattamenti di sua diretta competenza, effettuano operazioni di trattamento di dati personali siano formalmente "autorizzati" e siano **impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.**

Il Responsabile è tenuto, inoltre, a garantire il rispetto, anche da parte del personale assegnato alla struttura gestita, delle misure precauzionali individuate nei documenti (procedure, istruzioni operative, note ecc..) eventualmente adottati al fine di assicurare trasparenza ai processi ed agli adempimenti in materia di protezione dei dati personali, diffondere una più ampia cultura della riservatezza e perseguire una miglior tutela dei dati personali.

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.

La funzione di Responsabile del trattamento dei dati e attribuita personalmente e non è suscettibile di delega.

5.4 AUTORIZZATI O INCARICATI DEL TRATTAMENTO

Il Titolare o il Responsabile, qualora non sia già stato fatto, devono **nominare** gli **Autorizzati** o **Incaricati al trattamento** dei dati.

Gli incaricati sono le persone fisiche autorizzate dal Titolare o dal Responsabile a compiere operazioni di trattamento. In pratica, sono coloro che materialmente effettuano, attenendosi alle istruzioni impartite dal Titolare o dal Responsabile, le operazioni di trattamento di dati personali.

La designazione ad "incaricato" costituisce presupposto di liceità dei trattamenti dati effettuati; la nomina è effettuata per iscritto e individua l'ambito di trattamento consentito.

In generale, tutti coloro che trattano dati personali devono essere autorizzati e/o nominati incaricati del trattamento e quindi, nella fattispecie, non solo i dipendenti Avis, sia a tempo indeterminato che a tempo determinato, ma anche:

- **Amministrativo/contabile**: che visualizza e gestisce i dati associativi, necessari nell'ambito dello svolgimento della propria attività, riferiti ai soci donatori, soci aspiranti donatori o soci non donatori;
- **Volontari *(consiglieri, revisori dei conti e altri organismi associativi):*** che prestano la loro opera per il perseguimento di fini associativi e che trattano i dati associativi del donatore;

- **soci (donatori e non) e collaboratori*:*** che svolgono attività associative che comportino l'acquisizione e in generale il trattamento di dati personali, ad esempio: risposte a richieste telefoniche provenienti da donatori o aspiranti donatori, effettuazione di attività promozionali, chiamata del donatore;
- **Medico**: responsabile della seduta di raccolta, dell'attività donazionale e della selezione del donatore, segue il percorso clinico del donatore di sangue, visualizza e gestisce i dati relativi alla salute del donatore e ne raccoglie il consenso;
- **Infermiere**: dà supporto al Medico, addetto al prelievo ed all'assistenza sanitaria del donatore, visualizza e gestisce gli eventi dei donatori di sangue e raccoglie il consenso del donatore;
- **Assistente alla Sala Prelievi:** volontario incaricato per l'accoglienza e l'accompagnamento del donatore al "percorso donazionale"
- **Addetto al trasporto:** personale Incaricato per il trasporto delle unità prelevate e documentazione inerente la seduta di raccolta;

Il fatto che il rapporto fra l'incaricato e il titolare, sia inquadrato in un rapporto economico, oppure totalmente gratuito, è del tutto irrilevante

5.4.1 LA NOMINA DEGLI AUTORIZZATI O INCARICATI DEL TRATTAMENTO

Pur non prevedendo espressamente la figura dell'incaricato del trattamento, il regolamento non ne esclude la presenza, in quanto fa riferimento a persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4 par. 10). Tale figura è colui che effettua materialmente le operazioni di trattamento sui dati personali. Può essere solo una persona fisica e deve agire sotto la diretta autorità del Titolare o del Responsabile del trattamento.

La designazione è effettuata per iscritto con apposito atto redatto secondo il modello facsimile **(allegato B)** e individua l'ambito del trattamento consentito.

Si considera equivalente alla designazione esplicita anche la documentata assegnazione di un soggetto ad una unità operativa per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Agli Incaricati devono essere impartite le istruzioni per trattare i dati secondo le politiche della sicurezza e nella consapevolezza dei pericoli e delle responsabilità di trattamenti inadeguati e non autorizzati.

Ogni incaricato (sanitario, volontario, ausiliario, ecc.) è tenuto, oltre che a rispettare gli obblighi in materia di segreto d'ufficio anche al segreto professionale ed alla riservatezza, al pari del personale medico ed infermieristico (art. 9 del codice di deontologia medica del 3 ottobre 1998; art. 4 del codice deontologico per gli infermieri del maggio del 1999).

È opportuno sottolineare la responsabilità generale del Titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento al Regolamento, compresa l'efficacia delle misure di controllo e conservazione.

5.5 RESPONSABILE ED INCARICATI ESTERNI DEL TRATTAMENTO

Al fine di ovviare alla peculiare disciplina dettata dal Regolamento con riferimento alla comunicazione dei dati personali a terzi (legittima solo se prevista da una norma di legge o di regolamento), nei contratti o convenzioni con cui l'Associazione affida a terzi, persone fisiche o persone giuridiche, attività che comportano il trattamento di dati personali (es. in ipotesi di esternalizzazione di servizi) senza alcuna autonomia del terzo nella definizione di finalità e modi del trattamento che restano prerogativa esclusiva di **Avis**, quest'ultima nomina il terzo contraente come responsabile esterno dei trattamenti dei dati personali effettuati in forza del rapporto contrattuale o convenzionale.

Il Responsabile esterno è legittimato ad utilizzare, se indispensabili per l'espletamento dell'incarico affidato, i dati personali in possesso dell'Associazione.
Il Responsabile esterno risponde dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli art. 1218 e 1223 del Codice Civile.

Riguardo all'integrazione con i sistemi informativi, dal Titolare o dal Responsabile del Trattamento potranno essere designati come **Responsabili esterni del Trattamento dei dati** i fornitori:

- dei servizi informatici
- del software applicativo
- della gestione del server

con apposito atto di nomina che definisca gli ambiti, le finalità e i vincoli di trattamento.

Nel rispetto della normativa sulla privacy, i dati potranno essere trattati da **Incaricati esterni** – debitamente autorizzati - per svolgere specifici servizi elaborativi ed operazioni necessarie all'effettuazione dei servizi della rete, nei limiti strettamente pertinenti alle finalità del Sistema Informativo in oggetto.

5.6 DATA PROTECTION OFFICER (DPO)

L'Associazione dovrà valutare anche la necessità di nominare il ***Data Protection Officer*** (DPO), o **Responsabile della Protezione dei Dati** (**RPD**), figura prevista dall'art. 37 del Regolamento UE, il quale fornirà informazioni e consulenze sul trattamento e la sicurezza, coopererà con l'autorità di controllo e sorveglierà l'osservazione del Regolamento. La designazione del ***Data Protection Officer*** (DPO) anche se non obbligatoria è **sicuramente** opportuna in alcuni casi.

6. PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

I principi cardine alla base del trattamento sono:

Liceità e correttezza

Il trattamento deve avvenire in maniera lecita e corretta, informando l'interessato circa la raccolta, l'utilizzo e altri eventuali successivi trattamenti dei dati forniti. Il trattamento è lecito solo alle condizioni previste espressamente dall'art. 6 del Regolamento ovvero quando l'interessato ha espresso il proprio consenso (un **consenso informato**) al trattamento dei propri dati per una o più specifiche finalità, o quando il trattamento è necessario all'esecuzione di un **contratto** di cui l'interessato è parte, o ancora quando il trattamento è necessario per adempiere un **obbligo legale** a cui è soggetto il titolare del trattamento.

Trasparenza

Il trattamento, al fine di essere trasparente, deve avvenire con modalità predefinite e rese note all'interessato. Inoltre, devono essere facilmente accessibili e comprensibili le informazioni e le comunicazioni relative al trattamento (identità del titolare del trattamento, finalità del trattamento, diritti degli interessati…).

Limitazione delle finalità dei dati

I dati devono essere raccolti per finalità determinate, esplicite e legittime e successivamente devono essere trattati in una modalità che sia compatibile con tali finalità.

Minimizzazione dell'uso dei dati

Devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati.

Esattezza dei dati

Devono essere sempre esatti e aggiornati. Eventuali inesattezze devono essere tempestivamente rettificate ovvero i dati inesatti devono essere cancellati.

Limitazione della conservazione

I dati devono essere conservati per il tempo necessario al raggiungimento delle finalità per le quali sono trattati.

7. INFORMATIVA

Il Regolamento prevede che, all'atto della raccolta di dati personali, l'Interessato (la persona presso la quale i dati sono raccolti) debba ricevere una serie di informazioni, oralmente o per iscritto, previste agli artt. 13 e 14.

L'informativa è un momento fondamentale del trattamento dati, in quanto ne caratterizza la fase iniziale ed accompagna ogni sua fase. L'informativa ha, appunto, il compito di "informare" il soggetto, prima della raccolta dei suoi dati, su che fine faranno quelle informazioni (come saranno trattate, per quali scopi, con che impatto sulla sua privacy, con che tempi e limiti) e sui diritti che il soggetto potrà esercitare nei confronti di coloro che trattano quelle informazioni.

L'informativa deve essere precisa e dettagliata circa le finalità per cui viene posto in essere il trattamento. Nell'Informativa sono, inoltre, presenti tutte le informazioni essenziali all'esercizio dei diritti dell'interessato, come per esempio le informazioni di contatto del titolare e l'indirizzo e-mail per le comunicazioni che facilitino l'esercizio dei diritti e di una eventuale revoca del consenso.

Come precedentemente detto, l'informativa può anche essere data oralmente, ma in tal caso diventa difficile provare l'avvenuto adempimento in caso di contestazioni. Per questo motivo, soprattutto se si debbano effettuare trattamenti per i quali è necessario il consenso dell'interessato, è opportuno inserire l'informativa scritta nello stesso modulo del consenso, così da poter disporre di evidenza probatoria nel caso di eventuali contestazioni.

L'informativa è fornita con il modello (fac-simile) - Informativa-Consenso - di cui all'**allegato C** al presente documento, è può essere resa accessibile anche mediante affissione nei locali dell'Associazione.

Ogni qualvolta si debba effettuare un trattamento dati per finalità diverse da quelle contemplate nell'informativa o con modalità diverse da quelle esplicitate, sarà necessario provvedere alla modifica dell'informativa o alla redazione di un'apposita informativa da rendere agli interessati, nella quale siano riportati gli elementi minimi richiesti dall'artt.13 e/o 14 del Regolamento con riferimento allo specifico trattamento.

8 CONSENSO

Gli interessati devono avere la possibilità di prestare il proprio consenso. Ai sensi dell'art. 7 del Regolamento, il consenso deve essere espresso mediante dichiarazione o chiara azione positiva con la quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano.

Il consenso deve essere richiesto utilizzando un linguaggio semplice e chiaro, specificamente (per finalità) ed essere **chiaramente distinguibile, comprensibile e facilmente accessibile.**

Il Regolamento non prevede obbligatoriamente la forma scritta per il consenso. Tuttavia, considerato che il Titolare del trattamento, sempre ai sensi dell'art. 7, par. 1, ha l'onere di "*dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali*", è evidentemente raccomandata l'opportunità di provvedere all'acquisizione del consenso in forma scritta. Il consenso è espresso con lo schema (fac-simile) - Informativa-Consenso - di cui all'**allegato C**.

Il consenso si applica a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso deve essere prestato per tutte queste.

Deve essere chiaro anche il riconoscimento del diritto a revocare il proprio consenso in qualsiasi momento.

8.1 CONSENSO FACOLTATIVO

Il trattamento è considerato lecito quando è necessario:

- nell'ambito di un contratto o ai fini della sua conclusione o esecuzione;

- per adempiere ad un obbligo legale;
- per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Ricorrendo una delle predette ipotesi, il consenso non è necessario ed è sufficiente la consegna dell'informativa (con ricevuta che attesti la presa visione da parte dell'interessato), che attesta così l'importanza della propria funzione nell'ambito del trattamento dei dati personali.

Si ricade in queste condizioni ed il trattamento dei dati – previa informativa – è lecito a prescindere dal consenso quando, ad esempio, i dati debbono essere acquisiti e trattati nell'ambito della gestione di un contratto e conseguente rapporto di lavoro, mandato professionale ed ogni attività fisiologicamente connessa (a mero titolo esemplificativo e non esaustivo: instaurazione e gestione del rapporto di lavoro; elaborazione prospetti paga; adempimenti dichiarativi in materia contributiva e fiscale; gestione di infortuni e malattia, etc.)

8.2 CATEGORIE PPARTICOLARI DI DATI E CONSENSO

La normativa intende assicurare ai dati personali sensibili, suscettibili di creare discriminazioni di vario tipo nei confronti dei soggetti interessati, maggiore attenzione e protezione rispetto ai comuni dati personali. Infatti, così come indicato all'art. 9 del Regolamento, il consenso all'acquisizione dei dati sensibili deve essere esplicito. Lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

9. REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Titolare del trattamento e ciascun Responsabile del trattamento devono istituire un **Registro delle attività di trattamento** (**allegato D**), in forma scritta, svolte sotto la propria responsabilità che deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo (art. 30 del Regolamento).

Tale strumento consente di censire con precisione tutte le banche dati, di avere sotto controllo le finalità per le quali i trattamenti vengono svolti e altri elementi rilevanti per la valutazione del rischio.

Il registro deve contenere almeno le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento;
b) i dettagli inerenti le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) gli eventuali trasferimenti in Paesi terzi;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32, paragrafo 1.

10. ADEGUATEZZA DELLE MISURE ADOTTATE

Il Titolare del trattamento, tenendo conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche, all'atto del trattamento ovvero di determinare i mezzi del medesimo, adotta **misure tecniche e organizzative adeguate**, in modo da attuare efficacemente i principi di protezione dei dati e garantire nel trattamento i requisiti del Regolamento (art. 24 - 26 del Regolamento).

Ciò implica anche la verifica e l'eventuale necessità di adeguamento degli strumenti (hardware / software) attraverso i quali il trattamento viene effettuato.

11. VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DATI

Quando la valutazione di impatto indica che il trattamento presenta un rischio elevato per i diritti e le libertà delle persone fisiche, per le caratteristiche del trattamento o degli strumenti adottati per esso (ad

esempio novità tecnologiche, finalità, natura dei dati), prima di procedere al trattamento, il Titolare è tenuto a consultare l'autorità di controllo (art. 35 - 36 del Regolamento).

Al di fuori di tali esigenze specifiche non è un adempimento standard riferibile all'attività di **Avis**.

12. DIRITTI DELL'INTERESSATO

12.1 DIRITTO DI ACCESSO

L'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e l'accesso agli stessi ed alle informazioni.

Attenzione: il Titolare deve predisporre sistemi adeguati per l'esercizio dell'accesso

➔ la prima modalità per garantire agli interessati il diritto di accesso è **fare una buona informativa**

12.2 DIRITTO DI RETTIFICA

L'interessato ha il diritto di ottenere la **rettifica dei dati personali inesatti** che lo riguardano **senza ingiustificato ritardo**. L'interessato ha il diritto di ottenere **l'integrazione** dei dati personali **incompleti**, anche fornendo una dichiarazione integrativa (tenuto conto delle finalità del trattamento).

Attenzione: il Titolare deve predisporre sistemi adeguati per l'esercizio del diritto di rettifica e sistemi adeguati per assicurarsi l'esattezza dei dati e l'effettiva necessità dell'integrazione degli stessi

➔ la prima modalità per garantire agli interessati il diritto di accesso è **fare una buona informativa**

12.3 DIRITTO ALLA CANCELLAZIONE («DIRITTO ALL'OBLIO»)

L'interessato ha il diritto di ottenere dal titolare del trattamento **la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare** senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento**;**
c) l'interessato si oppone al trattamento per motivi connessi alla sua situazione particolare;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società.

L'interessato deve poter esercitare questo suo diritto con la stessa facilità con cui ha espresso il consenso al trattamento dei suoi dati.

Attenzione: Il titolare del trattamento **deve descrivere come garantisce il diritto alla cancellazione**

➔ ciò significa per il Titolare dover determinare in anticipo un periodo di conservazione dei dati e di avvalersi di alcune soluzione tecniche per apporre una «data di scadenza» a dati o gruppi di dati

12.4 DIRITTO ALLA LIMITAZIONE DEL TRATTAMENTO

L'interessato ha il **diritto di ottenere** dal titolare del trattamento la **limitazione del trattamento**, vale a dire di richiedere la sola conservazione.

Attenzione: Il titolare del trattamento **deve descrivere come garantisce il diritto alla limitazione del trattamento**

➔ ciò significa per il Titolare determinare mediante procedure, scritte in modo da essere trasparenti ed opponibili, l'adempimento dell'esercizio del **diritto di limitazione**

Diritto di reclamo all'Autorità di controllo:

L'interessato ha il diritto di proporre reclamo all'Autorità Garante per **ogni presunta violazione** del Regolamento.

12.5 DIRITTO ALLA PORTABILITÀ DEI DATI

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso o su un contratto ai sensi dell'art. 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.

13. DATA BREACH

Il Titolare e il responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguata al rischio.

Nel momento in cui dovesse esserci una violazione della sicurezza dei dati personali **Avis** dovrà procedere, senza ingiustificato ritardo:

- alla **notifica della violazione di dati personali all'Autorità di controllo**, senza ingiustificato ritardo e, dove possibile, entro 72 ore dal momento in cui ne sono venuti a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche (art.33).;
- alla **comunicazione della violazione di dati all'interessato**, quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche (art.34).

Con la nozione di **violazione dei dati personali** (c.d. "**personal data breaches**"), si intende: la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.

Con il termine **data breach** si intende, dunque, un **incidente di sicurezza** in cui dati personali, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Esempi di ***''data breach''***:

- **perdita accidentale**: ad esempio, data breach causato da *smarrimento di una chiavetta USB* contenente dati riservati;
- **furto**: ad esempio, data breach causato da *furto di un notebook o di un tablet* contenente dati confidenziali;
- **infedeltà aziendal**e: ad esempio, data breach causato da una *persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico*;
- **accesso abusivo**: ad esempio, data breach causato da un *accesso non autorizzato o non consentito ai sistemi informatici* con successiva divulgazione delle informazioni acquisite

14. SANZIONI

Secondo quanto riportato nell'art. 83, paragrafo 2 del Regolamento:

- la **violazione delle disposizioni relative agli OBBLIGHI dei Titolari e dei Responsabili** è soggetta a **sanzioni amministrative** pecuniarie fino a 10 milioni di euro, oppure per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore alla predetta cifra;
- la **violazione delle disposizioni relative ai DIRITTI degli interessati** è soggetta a **sanzioni amministrative** pecuniarie fino a 20 milioni di euro, oppure per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore alla predetta cifra.