IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Procedura GDPR

Autore: DPO / Supporto Specialistico
Rivisto da U.O. Privacy Trasparenza e Integrità
Accettato da: Direzione Generale

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1	01.10.2020	Prima versione	DPO
L'ultima revisione sostituisce qualsiasi revisione precedente.			

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi – Cotugno – CTO

PROCEDURA PER LA GESTIONE DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Sommario

CAPITOLO 1
INTRODUZIONE

Il General Data Protection Regulation (di seguito, "GDPR") è un Regolamento, redatto dalla Commissione Europea e pubblicato sulla "Gazzetta Ufficiale" dell'Unione Europea in data 4 maggio 2016, che ha il fine di armonizzare all'interno dell'UE le norme relative alla gestione dei dati personali.

Il presente documento si inquadra nel contesto degli aspetti inerenti alla gestione del Registro delle Attività di Trattamento, con lo scopo di descrivere le attività necessarie alla sua compilazione e successiva gestione.

Il Registro dei trattamenti dei dati è considerato il cardine centrale degli adempimenti nei modelli privacy che l'azienda dovrà adottare; esso è lo strumento di rappresentazione verso l'autorità garante del progetto privacy adottato e pertanto occorrerà porre la massima attenzione nella sua predisposizione e compilazione.

Esso deve offrire una fotografia dei trattamenti eseguiti presso un'organizzazione ed è fondamentale, perché costituisce la base per identificare e procedere a tutti gli altri adempimenti, serve a definire a tutto tondo l'organizzazione del Titolare sotto il profilo della protezione dei dati. Naturalmente, redatto una prima volta, deve essere aggiornato, affinché ne sia mantenuta l'aderenza alla effettiva realtà organizzativa.

Inoltre, non bisogna dimenticare che il Registro anche se sostanzialmente rappresenta un documento a valenza esterna (deve essere esibito su richiesta del Garante per documentare l'adempimento delle misure prescritte dal Regolamento e dalle altre disposizioni dell'ordinamento giuridico in materia di data protection), ha anche un ruolo interno di tipo sistemico in quanto, quale modello organizzativo "privacy", definisce le procedure per la condivisione delle informazioni in esso contenute tra i vari collaboratori/autorizzati, che debbono poter gestire con la dovuta consapevolezza le varie operazioni relative ai trattamenti assegnati.

1.1 FINALITÀ DEL DOCUMENTO

IL GDPR introduce la necessità da parte del Titolare del trattamento e, dove applicabile, del proprio rappresentante, di avere un Registro delle Attività di Trattamento (di seguito Registro dei Trattamenti) svolte sotto la propria responsabilità (Art. 30).

Scopo del presente documento è quello di fornire le linee guida per facilitare la redazione e l'aggiornamento del Registro dei Trattamenti, da parte della struttura sanitaria, come richiesto dal Regolamento Europeo.

Il Titolare del trattamento dati ha la responsabilità di mettere in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare la conformità al GDPR (art. 32 Regolamento UE 679/2016). Tali misure vanno aggiornate e riesaminate se necessario e devono essere preventive, devono tener conto dello stato dell'arte e dei costi di attuazione.

A tale proposito il Titolare del trattamento, in ottica di accountability, deve rivedere ed aggiornare i sistemi di gestione e gli strumenti informatici in uso rendendoli conformi al Regolamento UE 2016/679. Ciò richiede che tutte le UO della Struttura Sanitaria, ognuno per il proprio ambito di competenza in relazione al trattamento dovranno supportare il titolare ed il RDP/DPO nello svolgimento delle valutazioni di conformità al GDPR.

La redazione del Registro dei trattamenti è proprio uno dei principali adempimenti di accountability previsti dal Regolamento UE 2016/679; i contenuti di tale Registro sono elencati nelle lettere da a) a g) dell'art. 30.1.

1.1.1 DOCUMENTI DI RIFERIMENTO

Il presente paragrafo contiene la lista dei documenti di riferimento.

[1] Regolamento (UE) 2016/679 (GDPR)
[2] Template del Registro dei Trattamenti (in allegato)

1.2 GLOSSARIO

Acronimo/Definizione	Descrizione
GDPR	General Data Protection Regulation
RAT	Registro delle Attività di Trattamento
DPIA	Data Protection Impact Analysis
DPO	Data Processor Officer
RPD	Responsabile della Protezione dei Dati
UOC/UOSD	Unità Operativa Complessa/Unità Operativa Semplice Dipartimentale
Delegato interno al Trattamento dati	Soggetto interno all'Amministrazione, formalmente individuato, cui il Titolare attribuisce compiti e funzioni specificamente individuati nell'ambito delle operazioni di trattamento effettuate nell'ambito della struttura di diretta competenza.

Tabella 1–Glossario

CAPITOLO 2
REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

CAP. 2

Il Registro dei trattamenti è uno strumento fondamentale non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno di una organizzazione, ma è anche la fonte primaria di riferimento per lo svolgimento delle attività di analisi e valutazione degli impatti sulla privacy e sui rischi di sicurezza delle informazioni trattate.

Redigerlo implica l'esecuzione di una mappatura dei trattamenti di dati che consenta di acquisire le informazioni su finalità dei trattamenti, tipologie di interessati, categorie di dati personali e di destinatari dei medesimi (a vario titolo e, se del caso, anche in Paesi extra-UE) e - dove possibile, come precisa la disposizione - anche quelle concernenti i termini di cancellazione dei dati nonché una descrizione generale delle misure di sicurezza (tecniche ed organizzative) adottate per la loro protezione.

Ciò premesso, si comprende bene come la redazione del Registro dei trattamenti richiede tutta una serie di attività che vanno ben oltre quelle degli adempimenti legali e procedurali previsti dal Regolamento UE 2019/679 e che, affinché possano fotografare i singoli trattamenti posti in essere dal Titolare, necessitano di analisi, studi e riscontri puntuali. Fotografare i singoli trattamenti vuol dire anche analizzare il proprio sistema gestionale dei dati sia in termini di organizzazione e processi che in termini di applicazioni e infrastrutture al fine di valutare – per ogni trattamento gestito – i gaps rispetto alle richieste del GDPR e alla eventualità che un trattamento possa rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche e quindi la necessità di disporre una DPIA (valutazione d'impatto) dello stesso.

Tutto questo richiede:

- individuazione dei trattamenti posti in essere all'interno dell'Azienda;
- analisi delle problematiche legate al trattamento dei dati personali;
- individuazione dei trattamenti su server e su postazioni stand alone;
- responsabilizzazione del singolo delegato alla titolarità del trattamento dati;

- verifica della sussistenza delle misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato ai rischi;
- compilazione del Registro dei trattamenti dati come sommatoria dei trattamenti delle singole unità operative;
- supporto e formazione sull'attività di manutenzione del Registro;
- individuazione delle banche dati interessate dalle diverse attività di trattamento con il responsabile dei sistemi informativi aziendali e con il DPO;
- supporto al DPO per il monitoraggio della continua rispondenza tecnica delle misure di sicurezza.

I Delegati interni al trattamento dati (Direttori UU.OO.CC. e UU.OO.SS.DD.) sono tenuti a collaborare, per la mappatura dei trattamenti, anche ai fini del successivo aggiornamento.
Tutte le strutture dell'Azienda, ciascuna per il proprio ambito di competenza in relazione al trattamento effettuato, supportano il Titolare, l'Ufficio Privacy e il DPO nello svolgimento delle valutazioni di conformità al GDPR.
I Delegati segnalano le proposte di adeguamento necessarie a seguito di eventuali modifiche relative alle attività di trattamento, nonché degli eventuali mutamenti organizzativi o tecnici che riguardano i trattamenti di competenza effettuati, le modalità di svolgimento degli stessi, nonché le eventuali esternalizzazioni.
Ogni ulteriore trattamento posto in essere, o le eventuali modifiche intervenute (nei termini sopra indicati), deve essere pertanto comunicato al Titolare, al RPD/DPO ed all'Ufficio Privacy al fine di aggiornare il predetto Registro previa valutazione dell'impatto privacy.
La U.O.C. che si occupa della gestione dei sistemi IT, nello specifico provvede a riscontrare la conformità dell'utilizzo delle risorse IT e a verificare la conformità al GDPR dei software applicativi utilizzati e le modalità di accesso alle banche dati interessate.
Il suddetto percorso consente al Titolare, con cadenza periodica - mediante attività di ricognizione - di verificare, per il tramite dei Delegati Interni al trattamento, l'attualità del registro alle attività di trattamento svolte.

Le modalità operative secondo le quali tali attività dovranno svolgersi sono:

- ✓ analisi comparativa tra i trattamenti teoricamente individuati sulla base delle attività istituzionali della azienda e quelli da censire realmente sul campo. A tale proposito si avrà:
  - lo svolgimento di appositi incontri/interviste con i referenti aziendali responsabili delle unità operative decisionali, il DPO e l'ufficio privacy finalizzati al raggiungimento della definizione di un elenco di trattamenti consolidato e completo che fotografi in maniera realistica i trattamenti di dati personali svolti in Azienda;
  - la predisposizione di uno schema del Registro dei trattamenti elaborato sulla base delle informazioni raccolte nell'attività precedente.
- ✓ raccolta sul campo delle informazioni necessarie alla verticalizzazione del Registro nel contesto specifico dell'Azienda, al fine di individuare tutti gli elementi informativi necessari alla compilazione del Registro dei trattamenti. Questa attività sarà condotta attraverso:
  - la stretta collaborazione con il DPO e l'ufficio privacy con i quali condividere i criteri e gli eventuali strumenti utilizzati per la rilevazione dei dettagli informativi richiesti per la costruzione del Registro dei Trattamenti, come previsto dall'art. 30 del Regolamento.

Secondo il Regolamento (art. 30 par. 1), il Registro delle Attività di Trattamento deve contenere perlomeno le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;

- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, par 1.

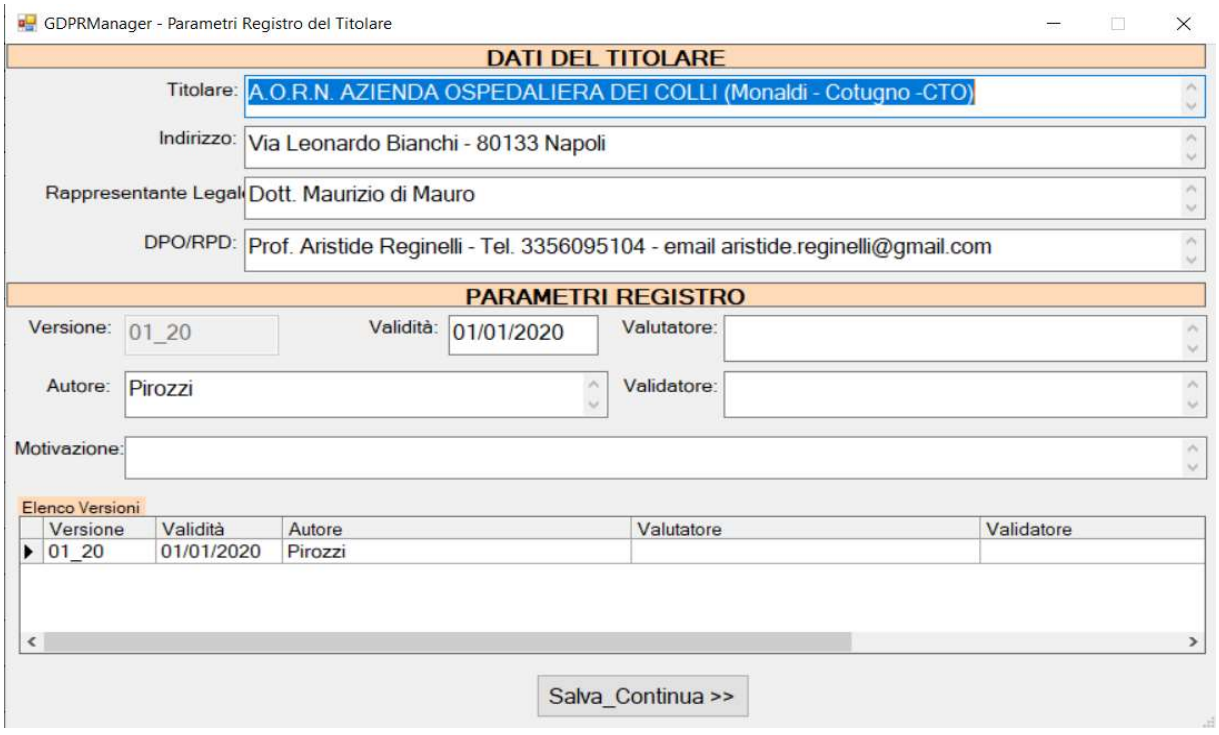
Nella fattispecie il Registro dei Trattamenti verrà prodotto in Formato Microsoft Excel; esso verrà generato da un applicativo software proprietario, semplice e intuitivo, che offre tutta una serie di facilitazioni e suggerimenti per una sua corretta compilazione. Tale software utilizza come data-Input l'"Elenco Base dei Trattamenti" censiti durante le attività di ricognizione e mappatura prime descritte, corredato da tutta una serie di tabelle da cui selezionare le definizioni opportune. Elenco base e tabelle sono a loro volta strutture in formato Excel che il software in questione gestisce come tabelle a tendina da cui selezionare le definizioni opportune. Ovviamente sarà sempre possibile accettare ex-novo eventuali definizioni non previste nelle liste predefinite.

Il Registro dei Trattamenti in formato Excel che verrà generato è strutturato, come evidenziato nel Template allegato, e come di seguito descritto nelle seguenti sezioni:

1. Informazioni generali
2. Elenco dei Trattamenti

2.1 INFORMAZIONI GENERALI

Questa sezione è propedeutica alla compilazione vera e propria del Registro e oltre ai dati del Titolare comprende una serie di parametri relativi alla release, ai dati dell'autore e dei soggetti preposti alla valutazione e validazione. Una volta validato il documento Excel che rappresenta il Registro verrà bloccato e protetto da apposita password di dominio del soggetto che opera la validazione.



Eventuali modifiche o aggiornamenti del Registro dei Trattamenti, precedentemente validato, verranno gestiti come versioni successive, mantenendo inalterate le versioni precedenti; un apposito campo "Motivazioni" potrà servire per descrivere i motivi della redazione di una nuova versione.

Tale modalità consentirà al Titolare del trattamento di dimostrare in continuità la conformità al GDPR (art. 32 Regolamento UE 679/2016), ma principalmente di disporre di un quadro aggiornato dei trattamenti in essere all'interno della sua organizzazione.

Nello specifico nella prima sezione sono esplicitate alcune informazioni generali quali:

- **Dati del Titolare**: devono essere indicati i dati identificativi del Titolare (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) e i suoi dati di contatto;
- **Dati del Referente Privacy** (qualora nominato): devono essere indicati i dati identificativi del Responsabile dell'Ufficio Privacy (persona fisica nominata dal Titolare con la responsabilità di svolgere i compiti a lui assegnati) e i suoi dati di contatto;
- **Dati del DPO** (qualora nominato): devono essere indicati i dati identificativi del Responsabile della Protezione dei Dati (RPD o DPO)e i suoi dati di contatto;
- **Data di inizio validità**: deve essere indicata la data di creazione del Registro dei Trattamenti;
- **Data di aggiornamento**: deve essere indicata l'ultima data in cui il Registro dei Trattamenti è stato aggiornato.

Nella

Figura 1sono mostrati i campi della sezione così come verranno riportati sul Registro.

TITOLARE:	
Indirizzo:	
Legale Rappresentante:	
Versione:	
Validità:	

DPO:		
Autore:		
Valutatore:		
Validatore:		

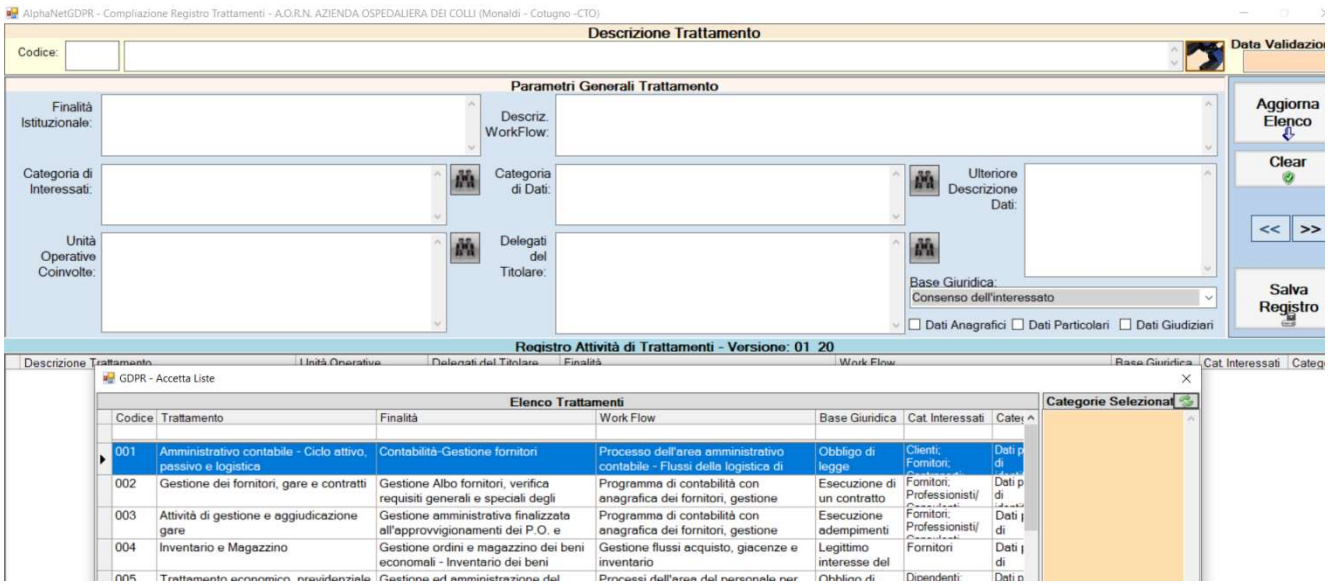
Figura 1- Informazioni Generali

2.2 ELENCO DEI TRATTAMENTI

Il Registro dei trattamenti è uno degli adempimenti cogenti previsti dal GDPR e deve essere tenuto in forma scritta o anche in formato elettronico e messo a disposizione dell'autorità di controllo qualora richiesto.

Il Registro dei Trattamenti, corretto ed aggiornato nel tempo, costituisce una significativa evidenza della responsabilizzazione del Titolare, e costituisce l'elemento basilare per un approccio razionale ed esaustivo alla gestione della privacy, in quanto fornisce un quadro sinottico dei trattamenti posti in essere dall'organizzazione, da utilizzare come fonte di riferimento per ogni attività di valutazione degli impatti e dei rischi privacy.

Di seguito si riportano le interfacce del software di cui sopra, e la definizione dei campi presenti nella sezione "Elenco Trattamenti", nella quale vengono esplicitate le informazioni relative a ciascun trattamento:



Nelle interfacce sopra illustrate è possibile identificare nel dettaglio le colonne che compongono e descrivono ogni singolo trattamento:

Denominazione del Trattamento	Base giuridica del trattamento	Paese Terzo Extra UE
Finalità del trattamento	Tipologia di dati: Personali, Particolari, Giudiziari	Garanzie adottate verso paesi Extra UE
Descrizione Workflow processo	Modalità di archiviazione dati	Localizzazione/Ubicazione dati cartacei
Categorie di Interessati	Modalità di trattamento dati	Tipo-Nome DB/Software applicativo

Categoria di Dati personali	Periodo di conservazione	Localizzazione/Ubicazione Server
Descrizione categoria di dati	Modalità di raccolta Consenso	Misure di sicurezza organizzative
Unità Operative coinvolte	Soggetti a cui possono essere comunicati i dati	Necessità DPIA
Delegati del Titolare (Responsabili UU.OO.)	Ente terzo/ Responsabile al trattamento	Note

2.2.1 DENOMINAZIONE TRATTAMENTO

Si definisce "trattamento" (art. 4) "*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*".

In questo campo deve essere riportato l'identificativo del Trattamento selezionandolo dall'"Elenco Base dei Trattamenti" censiti durante le attività di ricognizione e mappatura prime descritte, oppure, laddove non presente in tale elenco, può essere a compilazione libera. In tal caso, a completamento delle informazioni ad esso associate, verrà aggiunto all'elenco base.

2.2.2 FINALITÀ DEL TRATTAMENTO

In questo campo deve essere inserita una breve descrizione delle finalità del trattamento. Il campo è attinto anch'esso dall'elenco base dei trattamenti con possibilità di modifica o compilazione libera. In Figura 2 è riportato un elenco, ovviamente non esaustivo, di possibili finalità. Ovviamente quando si tratta di un nuovo Trattamento che si aggiunge all'elenco suddetto, la finalità specificata verrà salvata insieme al trattamento.

Figura 1

Esempi Finalità
Rilascio esenzione
Assistenza sanitaria
Gestione del personale
Gestione di assicurazione sanitaria
Assicurazione incidenti sul lavoro
Gestione l. 81/2008
Controllo accessi
Prevenzione frodi
Sicurezza fisica
Gestione del contenzioso
Gestione fornitori
Albo fornitori
Gestione Clienti
Anagrafica clienti
Contabilità
Gestione crediti
Insurance Management fuoco, incidenti e rischi vari
Pianificazione delle attività
Pubbliche relazioni
Ricerche di mercato
Customer Care
Marketing
Direct Marketing
Informazioni commerciali
Analisi generale clientela
Ricerca storica
Ricerca statistica
Altro

Figura 2-Esempi di finalità

2.2.3 DESCRIZIONE WORKFLOW PROCESSO

In questo campo deve essere inserita una breve descrizione del trattamento ed in particolare del processo con cui questo viene gestito. Il campo è a compilazione libera.

2.2.4 CATEGORIE DI INTERESSATI

In questo campo deve essere riportata la categoria di interessati del trattamento. L'interessato è una persona fisica identificata o identificabile, direttamente o indirettamente, con delle informazioni quali il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o con uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Il campo è tabellato ma può essere anche compilato liberamente. La tabella, non esaustiva, è riportata in Figura :

Categorie di Interessati
Assistiti/Pazienti
Familiari
Dipendenti
Professionisti/Consulenti
Collaboratori
Clienti
Fornitori
Utenti
Controparti
Associati
Appartenenti all'organizzazione
Membri di organismo di amministrazione
Membri di organismi di controllo
Revisori
Soci
Appartenenti a pubblica amministrazione
Altro (specificare)

Figura 3- Categoria di interessati

2.2.5 CATEGORIA DI DATI PERSONALI

In questo campo deve essere riportata la categoria di dati utilizzata nel trattamento (es. anagrafica, dati sanitari, dati finanziari). Il campo è attinto anch'esso dall'elenco base dei trattamenti; in Figura 4 è riportato un elenco, ovviamente non esaustivo, di possibili finalità.

Categoria di Dati
Dati personali di identificazione
Dati sullo stato di salute
Dati che rivelano l'origine razziale o etnica
Dati che rivelano opinioni politiche
Dati che rivelano convinzioni religiose o filosofiche
Dati che rivelano l'appartenenza sindacale
Dati sulla vita sessuale o sull'orientamento sessuale
Dati giudiziari relativi a condanne penali e reati, articolo 10 del GDPR
Dati genetici per l'identificazione univoca di una persona
Dati biometrici per l'identificazione univoca di una persona
Dati genetici nel contesto di uno screening, un esame di ereditarietà
Dati personali protetti dal segreto professionale
Dati che, in generale, possono aumentare il rischio potenziale per i diritti e le libertà delle persone
Dati di comunicazione e identificazione elettronica
Dati di geolocalizzazione
Dati finanziari
Debiti, spese, solvibilità
Prestiti, mutui e crediti
Dettagli assicurativi
Dettagli sulla pensione
Dati professionali
Convenzioni e accordi
Permessi lavorativi
Informazioni personali
Situazione militare
Stato dell'immigrazione
Descrizione fisica
Stile di vita
Contatti sociali
Dati Patrimoniali
Mandati pubblici
Matrimonio o forma attuale di convivenza
Storia civile
Dettagli di altri membri della famiglia
Attività ricreative e interessi
Affiliazioni (diverse da quelle professionali, politiche o sindacali)
Curriculum accademico e professionale
Qualifiche professionali
Affiliazione / partecipazione a organizzazioni professionali
Presenza e disciplina
Medicina del lavoro
Numero di identificazione nazionale
Partecipazione a gruppi di pressione / organizzazioni attiviste
Registrazioni di immagini
Immagini di sorveglianza
Dati relativi alla prestazione lavorativa
Altro

Figura 4- Categoria di interessati

2.2.6 DESCRIZIONE CATEGORIA DI DATI

In questo campo deve essere descritta con maggiore dettaglio la categoria inserita nel campo precedente, indicando i dati personali che la compongono (es. nome, cognome, indirizzo, diagnosi clinica, numero conto corrente). Il campo è a compilazione libera.

2.2.7 UNITÀ OPERATIVA

In questo campo deve essere inserita l'Unità Organizzativa dell'azienda, il servizio o il Presidio in cui viene svolto il Trattamento. Anche per questo campo è prevista una lista, nella fattispecie, dell'organigramma aziendale dalla quale selezionare la o le UU.OO. che effettuano il trattamento in questione (più unità Operative possono effettuare lo stesso trattamento, come ad esempio il trattamento di Degenza). In tale campo vanno indicate tutte le altre UU.OO. che concorrono al trattamento.

2.2.8. DELEGATI DEL TITOLARE

In questo campo vanno indicati i responsabili (Delegati interni del Titolare) delle UU.OO. che concorrono al trattamento in questione. Anche a questo campo è associata la lista dell'organigramma aziendale. Ovviamente esso, come anche quello precedente, possono essere a compilazione libera qualora la tabella dell'organigramma aziendale dovesse essere non aggiornata.

2.2.9 BASE GIURIDICA DEL TRATTAMENTO

In questo campo devono essere riportati i principi di liceità del trattamento come previsto dall'Art. 6 par. 1, dall'Art. 9 e dall'Art. 10 del GDPR. Il campo deve essere compilato attraverso la scelta di una voce dal menu a tendina riportato in Figura :

Elencco Base Giuridica
Consenso dell'interessato
Finalità di cura della salute
Trattamento ex art. 9 lett. d) GDPR
Legittimo interesse del Titolare
Esercizio obblighi in materia di diritto del lavoro
Esercizio obblighi in materia di protezione sociale
Esecuzione di un contratto
Esecuzione adempimenti precontrattuali
Obbligo di legge
Salvaguardia interessi vitali dell'Interessato
Dati personali resi pubblici dall'Interessato
Esecuzione compiti di interesse pubblico
Interesse pubblico per sanità pubblica
Ricerca storica o statistica
Esistenza del segreto professionale
Esercizio di pubblici poteri
Altro (specificare)

Figura 5- Base giuridica del trattamento

2.2.10 TIPOLOGIA DI DATI

I dati personali sono classificati nelle seguenti tipologie:

- **Dati personali**: 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 (vedi Art.4 par.1).

- **Dati particolari (o sensibili)**: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati giudiziari**: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Per indicare la tipologia di dati trattati dallo specifico trattamento è necessario apporre una "x" ad uno o più di questi campi.

2.2.11 MODALITÀ DI RACCOLTA DEI DATI

In questo campo deve essere riportato il formato con il quale vengono raccolti i dati del trattamento, attraverso la scelta di una voce dal menu a tendina riportato in Figura 6:

Modalità di raccolta dati
N/A
Cartaceo
Digitale
Cartaceo e digitale
Registrazione telefonica
Digitale e registrazione telefonica

Figura 6- Modalità di raccolta dati

2.2.12 MODALITÀ DI GESTIONE DEI DATI

In questo campo deve essere riportata la modalità con la quale vengono gestiti i dati del trattamento, attraverso la scelta di una voce dal menu a tendina riportato in 7:

Modalità di gestione dati
N/A
Automatizzata
Non automatizzata
Semiautomatizzata

Figura 7- Modalità di gestione dati

2.2.13 MODALITÀ DI ARCHIVIAZIONE DEI DATI

In questo campo deve essere riportato il formato con il quale vengono archiviati i dati del trattamento, attraverso la scelta di una voce dal menu a tendina riportato in Figura 8:

Modalità di conservazione dati
N/A
Cartaceo
Digitale
Cartaceo e digitale
Registrazione telefonica
Digitale e registrazione telefonica

Figura 8- Modalità di conservazione dati

2.2.14 PERIODO DI CONSERVAZIONE

In questo campo, a compilazione libera, devono essere riportati i termini ultimi previsti per la cancellazione dei dati personali trattati. Il periodo di conservazione dei dati deve essere strettamente correlato allo scopo perseguito con il trattamento, ovvero deve rispettare i termini di legge qualora esistenti. Il principio di limitazione del periodo di conservazione dei dati personali è riportato in diversi punti del Regolamento UE e dei considerando allegati.

Ad esempio, al considerando 39 si dice che: "*il titolare deve assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. Ovvero i dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati per sonali inesatti siano rettificati o cancellati*."

Contestualmente, quale eccezione del principio anzidetto, al considerando 65 viene riportato testualmente: "… *Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria".*

Ciò premesso occorre precisare che non esistono, al momento, criteri ufficiali volti a stabilire in modo uniforme modalità e tempi di conservazione dei dati personali; tuttavia possono essere valutati alcuni parametri quali:

- **gli obblighi di legge** (normative nazionali ed internazionali);
- le **pronunce giurisprudenziali**-provvedimenti dell'Autorità, le indicazioni fornite dalle Associazioni di categoria, linee guida per le PA, o altri soggetti in grado di indicare elementi che facilitino la conservazione;
- i **contributi apportati dalla dottrina;**
- la **casistica** che pone al centro la tutela dell'interessato, e la salvaguardia dei contenuti degli archivi storici.

Nello specifico il Garante con il provvedimento 55 del 17 marzo 2019 ha fornito alcuni chiarimenti in merito ai tempi di conservazione per alcuni trattamenti specifici in ambito sanitario, quali:

- documentazione inerente agli accertamenti effettuati nel corso delle **visite per il rilascio del certificato di idoneità all'attività sportiva agonistica**: **5 anni**;
- **documentazione iconografica radiologica**: **10 anni**;
- **cartelle cliniche e referti**: **durata illimitata**.
- **Sperimentazioni cliniche**: **7 anni.**
  I documenti essenziali relativi allo studio (compresa la documentazione medica riferita ai singoli individui) devono essere conservati presso il promotore e i centri partecipanti per almeno sette anni dopo il completamento della sperimentazione; ovvero per un periodo di tempo considerevolmente più lungo in conformità alla disciplina applicabile o agli accordi intervenuti tra il promotore medesimo e centri partecipanti (art. 18 d.lg. n. 200/2007; d.lg. n. 219/2006, all. 1, punto 5.2, lett. c); d.m. 15 luglio 1997, all. 1/4B, punti 4.9.4 e 4.9.5 e all. 1/5A, punti 5.5.11 e 5.5.12).

Resta comunque inteso che nel caso in cui, invece, i tempi di conservazione di specifici documenti sanitari non siano stabiliti da una disposizione normativa, il titolare del trattamento, in virtù del principio di

responsabilizzazione, dovrà individuare tale periodo in modo che i dati siano conservati, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati (principio di limitazione della conservazione, art. 5, par. 1, lett. e) del Regolamento) e indicare tale periodo (o i criteri per determinarlo) tra le informazioni da rendere all'interessato.

2.2.15 SOGGETTI A CUI POSSONO ESSERE COMUNICATI I DATI

Si definisce destinatario, l'insieme dei quali costituisce l'ambito di comunicazione: "la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento".

In questo campo deve essere riportata la categoria di destinatari a cui i dati personali sono stati o saranno comunicati. Il campo è a compilazione libera ma è possibile far riferimento ad alcuni esempi non esaustivi di ambiti di comunicazione riportati in Figura 9:

Ambito di comunicazione
Amministrazioni pubbliche
Amministrazioni finanziarie
Istituti di Previdenza
Organi di giustizia e di polizia
Servizi pubblici
ANAC
Banche e compagnie assicurative
Consulenti professionisti dell'Interessato
Altri soggetti che hanno rapporti con l'Interessato
Datore di lavoro
Imprese private
Societa di marketing
Fornitori di servizi informatici
Fornitori di servizi amministrativi e contabili
Piattaforme di elaborazione
Altro (specificare)

Figura 9- Esempi di Categorie di destinatari

2.2.16 RESPONSABILE DEL TITOLARE/CONTITOLARE

Il GDPR definisce Responsabile (ex art. 28) "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

In questo campo devono essere riportati i dati identificativi e di contatto del/i Responsabile/i eventualmente presente/i per lo specifico trattamento o dell'ente terzo, persona fisica o giuridica che tratta dati per contro del titolare del trattamento ma che non viene nominato Responsabile.

In tale campo, qualora il soggetto in questione si configura secondo l'art 26 del GDPR (1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento) va annotata chiaramente la condizione di contitolarità. E ciò in quanto essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

In questo campo devono essere riportati i dati identificativi e di contatto del/i contitolare/i eventualmente presente/i per lo specifico trattamento. Il campo è a compilazione libera.

2.2.17 MODALITÀ DI CONSENSO

Si definisce "consenso" (art.4): "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*".

In questo campo devono essere riportate le caratteristiche del consenso, qualora venga raccolto, attraverso la scelta di una voce del menu a tendina riportato in **Errore. L'origine riferimento non è stata trovata.**:

Consenso
N/A
Comportamentale
Espresso
Per iscritto
Documentato
Altro

Figura 3- Consenso

2.2.18 PAESI TERZI EXTRA UE VERSO I QUALI POSSONO ESSERE TRASFERITI I DATI

In questo campo deve essere indicato il paese terzo o l'organizzazione internazionale Extra UE verso cui si ha l'eventuale trasferimento dei dati. Il campo è a compilazione libera.

A tale proposito si chiarisce che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, anche se Extra UE, è ammesso se la Commissione UE ha stabilito che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato (Art. 45 comma 1 Capo V del Regolamento GDPR). **In tal caso il trasferimento non necessita di autorizzazioni.**

Nel caso contrario invece, ovvero in assenza di parere positivo da parte della Commissione UE, occorre che il Responsabile Esterno che effettua il trasferimento, fornisca in proprio le garanzie adeguate e venga assicurato che gli interessati possano esercitare i propri diritti utilizzando mezzi di ricorso effettivi.

Le garanzie necessarie vanno indicate al successivo campo.

2.2.19 GARANZIE ADOTTATE PER IL TRASFERIMENTO (Capo V GDPR)

In questo campo vanno indicate le garanzie, secondo la Commissione Europea per la Protezione dei Dati, offerte dal paese terzo in questione. Il campo è selezionabile da un elenco riportato nella Figura 12.

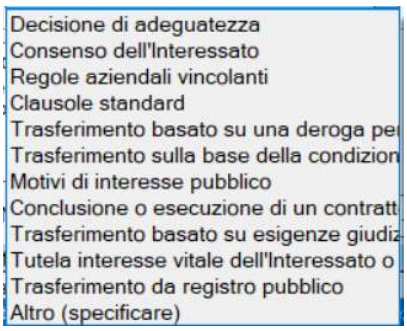


Figura 42 – Elenco Garanzie extra UE

2.2.20 LOCALIZZAZIONE/UBICAZIONE DATI CARTACEI

In questo campo devono essere riportate la ubicazione degli ambienti e la descrizione dei dispositivi fisici dove vengono custoditi e archiviati i dati cartacei (armadi con o senza chiusura, scaffali, etc.) Il campo è a compilazione libera.

2.2.21 TIPO DB/SOFTWARE GESTIONALI

In questo campo deve essere riportato il nome del data base nel quale sono memorizzati i dati relativi al trattamento e l'applicativo che li elabora. Il campo è a compilazione libera, tuttavia viene fornito un elenco degli Asset IT da cui selezionare quelli desiderati. Nella sottostante figura 13 è riportato, a titolo esemplificativo e raggruppato per area funzionale, il suddetto elenco riferito allo stato attuale; ovviamente laddove non si dovessero conoscere le informazioni da indicare in tale campo si può ricorrere al supporto della U.O.C Sistemi Informativi che, tra l'altro, dovrà provvedere a segnale all'Ufficio Privacy, previa attestazione di conformità al GDPR, l'introduzione di nuovi applicativi. **Ad ogni modo, l'elenco complessivo e aggiornato, sia per quanto riguarda gli applicativi di nuova adozione che la integrazione o la dismissione di quelli in uso, unitamente alla indicazione del fornitore e produttore, è contenuta nel "Registro delle attività di Trattamento".**

Descrizione Asset IT	**Ubicazione/Sistema BackUp e Restore**
MODULI *AREAS* AREA SANITARIA (TIM / ENGINEERING): • AREAS: X-MPI - Anagrafe Centrale; CUP - CUP Aziendale; WINSAP - Anatomia Patologica; ELIOT - Gestione Trasfusionale; ADT - Movimentazione Ospedaliera; PS - Pronto Soccorso; Rilevazione Spese Sanitarie. **DBMS:** Data Base Oracle	DB su server Farm sala CED locali SIA Monaldi; Sistema automatizzato backup/restore su Data Protector HP a cassette presso SIA monaldi
MODULI *ASAP* AREA SANITARIA (TIM / NEXERA): • ASAP SIO: Gestione Ambulatorio; Day Service; Gestione Reparto; Cartella Clinica; Ciclo del Farmaco; Preospedalizzazione; Blocco Operatorio; • Gestione Intramoenia; • Gestione Liste di Attesa; • RIS-PAC - Radiologia; • LIS - Portale Referti. **DBMS:** Data Base Oracle	DB su server Farm sala CED locali SIA Monaldi; Sistema automatizzato backup/restore su Data Protector HP a cassette presso SIA monaldi
MODULI LABORATORIO (TIM / DEDALUS): • DIAMANTE: Laboratori Biochimica Clinica, Virologia, Microbiologia, Patologia Clinica; • CALEIDO: Gestione Piattaforma Laboratori; • PARMA GT: Diagnostica Specialistica-Anagrafica a valore INR (TIM/WERFEN)	
QUANI-SDO (BIM ITALIA – GPI): • QUANI-SDO: Monitoraggio SDO **DBMS:** Data Base Oracle/SQL Server	DB su server Farm sala CED locali SIA Monaldi; Sistema automatizzato

GROUPER SERVER (3M): • Calcolo DRG	backup/restore su Data Protector HP a cassette presso SIA monaldi
MODULI *AREAS* AREA AMMINISTRATIVA (TIM / ENGINEERING): • AREAS HR: Gestione Human Resource; Gestione Giuridico Matricolare; Dotazione Organica; Fascicolo Dipendenti; Gestione Economica; Gestione Presenze (Ri.Pre.Sa); Portale Dipendente • SIOPE+: Gestione Mandati Pagamento; • Data Warehouse; SPAGOBI4; • PAGOPA+ENGPAY. **DBMS:** Data Base Oracle Gestito da TIM.	DB su server Farm sala CED locali SIA Monaldi; Sistema automatizzato backup/restore su Data Protector HP a cassette presso SIA monaldi
ALTRI MODULI AMMINISTRATIVI: • SIAC-SAP: Ciclo Attivo e Passivo Aziendale (**So.Re.Sa**); • GeCo: Gestione Concorsi (**Inaz Srl**); • Sinfopres: Flussi Regionali(**So.Re.Sa**) • LAPIS: Protocollo Informatico; Document Management System; Gestione Delibere e Determine; Gestione Trasparenza DLgs 33/13 e Anticorruzione l. 190/2012; Gestione Fascicolo di Liquidazione	DB su server Farm sala CED locali SIA Monaldi; Sistema automatizzato backup/restore su Data Protector HP a cassette presso SIA monaldi
INGEGNERIA CLINICA: • EXTENSA: Refertazione Emodinamica e Ecocardio (**Esaote**); • ENDOX: Servizio Endoscopia (**Olympus**). • TALETE WEB: Rischio Clinico (**Helathcare Engineering Service SRL**)	
PIATTAFORME WEB: • SANIARP Piattaforma Regionale; • Portale Fiore SIAC (**So.Re.Sa**); • Portale AIFA Registri di monitoraggio farmaci (**AIFA**).	

Figura 53 – Elenco Risorse IT

2.2.22 LOCALIZZAZIONE/UBICAZIONE SERVER

In questo campo deve essere riportato l'allocazione fisica dei server dove risiedono i DB e gli applicativi software. Esso è abbinato al campo precedente ma può essere dettagliato maggiormente mediante compilazione libera.

2.2.23 MISURE DI SICUREZZA ORGANIZZATIVE

Il campo in questione e quello successivo hanno lo scopo di rispondere all'art. 32 del GDPR, ovvero: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:*

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*."

A tale proposito gli elenchi riportati nelle Figure 14 e 15 consentono di scegliere le eventuali misure messe in atto dal Titolare a protezione dei dati relativi al trattamento in questione, fermo restando che è possibile definire liberamente eventuali altre misure o meglio specificare quelle indicate nelle suddette tabelle.

Ciò premesso, In questo campo devono essere riportate, ove possibile, le misure di sicurezza organizzativa adottate a protezione del trattamento. Il campo è a compilazione libera ma possono essere riportatele definizioni presenti nella tabella riportata in Figura 14.

Misure Organizzative
Nomina per iscritto Delegati ed Incaricati
Nomina per iscritto Responsabili esterni
Adozione Regolamenti e Procedure aziendali Privacy
Istruzioni scritte per il trattamento
Formazionedel personale
Accesso fisico e logico locali controllato
Procedura modifica automatica credenziali
Dati Cartacei conservati in buste/contenitori sigillati
Armadi muniti di serratura con chiave
Stanze munite di serratura con chiave
Casseforti con chiave
Altro (specificare)

Figura 14- Misure di sicurezza organizzativa

2.2.24 MISURE DI SICUREZZA TECNICA

In questo campo devono essere riportate, ove possibile, le misure di sicurezza tecnica adottate a protezione del trattamento. Il campo è a compilazione libera ma possono essere riportati le definizioni presenti nella tabella riportata in Figura 15.

Misure Tecniche
Autenticazione con User & Password
Autenticazione con caratteristiche biometriche
Autenticazione con Badge magnetici
Attivazione profili di autorizzazione (accesso parzializzato ai programmi aziendali)
Cifratura dei dati/pseuodonimizzazione
Installazione Sistemi antivirus/antimalware
Controllo automatico sistemi antivirus/antimalware
Monitoraggio centralizzato dei controlli antivirus/antimalware
Installazione strumenti controllo perimetrale antintrusione (Firewall)
Installazione Sistemi di intrusion detection (IDS/IPS)
Controllo dei flussi dei dati all'interno della rete aziendale (DLP-Data Loss Prevention)
Attivazione sistemi di vulnerability assessment/penetration test
Sistema di Backup e Restore
Definizione procedura di disaster recovery (business continuity)
Protezione accesso locali custodia Backup
Protezione accesso locali CED
Altro (Specificare)

Figura 6- Misure di sicurezza tecnica

2.2.25 NECESSITÀ DPIA

L'art. 35 cita: "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno*".

Qualora si ritenga che il trattamento presenti dei rischi elevati (per esempio perché tratta dati ultra-sensibili), compilare tale campo scegliendo la voce dal menu a tendina riportante:

- Non Richiesta;
- In Valutazione;
- Da Avviare;
- In Progress;
- Terminata.

2.2.26 NOTE

In questo campo è possibile riportare le eventuali note in riferimento ad uno qualsiasi dei campi precedenti ovvero i riferimenti a documenti che supportano quanto inserito. Il campo è a compilazione libera.

CAPITOLO 3
ALLEGATI

3.1 DOCUMENTAZIONE ALLEGATA

Allegato n. 1	**Template del Registro dei Trattamenti**