Provincia di Pisa

Organizzazione
DR. LUIGI PUCINO

Titolare del Trattamento dei Dati personali

DR. LUIGI PUCINO

DR. LUIGI PUCINO

Elaborato

REGISTRO DEL TRATTAMENTO

Redatto in base alle disposizione di cui al articolo 30 del
GDPR - General Data Protection Regulation
Regolamento EU 2016/679

Il Titolare del Trattamento dei Dati personali

Data : 24/05/2018

Capitolo 1
REGISTRO DEL TRATTAMENTO

1.1 Scopo

Il presente Registro del Trattamento è redatto per monitorare tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016. Inoltre costituisce un valido strumento per la adozione delle misure idonee previste dall'articolo 30 del GDPR.
Grazie al presente Registro del Trattamento è possibile monitorare e ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.
Considerando 82 - Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.

1.2 Campo di applicazione

Il Registro del Trattamento definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Registro del Trattamento riguarda il trattamento di tutti i dati personali:

- Generici
- Biometrici
- Relativi alla Salute
- Relativi a Opinioni Politiche
- Relativi all'orientamento e alla vita sessuale dell'individuo
- Giudiziari

Il Registro del Trattamento si applica al trattamento di tutti i dati personali per mezzo di:

□□ Strumenti elettronici di elaborazione
□□ Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il Registro del Trattamento deve essere tenuto aggiornato dai Responsabili del trattamento, approvato dal Titolare del Trattamento, conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.3 Riferimenti normativi

Articolo 30
Registri Delle Attività Di Trattamento
1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
   a) 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;
   b) le finalità del trattamento;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali; 4.5.2016 L 119/50 Gazzetta ufficiale dell'Unione europea IT;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) 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;
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'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
   a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
   b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
   c) 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;
   d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

1.4 Definizioni

Di seguito si riportano le principali definizioni usate in accordo con l'art. 4:

1.4.1 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;

1.4.2 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;

1.4.3 Limitazione di trattamento

Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

1.4.4 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;

1.4.5 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;

1.4.6 Archivio

Qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

1.4.7 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;

1.4.8 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;

1.4.9 Destinatario

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;

1.4.10 Terzo

La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

1.4.11 Consenso dell'interessato

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;

1.4.12 Violazione dei dati personali

La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

1.4.13 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;

1.4.14 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;

1.4.15 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;

1.4.16 Stabilimento principale

- per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
- con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

1.4.17 Rappresentante

La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

1.4.18 Impresa

La persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

1.4.19 Gruppo imprenditoriale

Un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

1.4.20 Norme vincolanti d'impresa

Le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; 21) «autorità di controllo»:l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

1.4.21 Autorità di controllo interessata

Un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

1.4.22 Trattamento transfrontaliero

- trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
- trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

1.4.23 Obiezione pertinente e motivata

Un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

1.4.24 Servizio della società dell'informazione

Il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1);

1.4.25 Organizzazione internazionale

Un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

1.5 Revisioni

INDICE DELLE REVISIONI					
Rev	Data	Descrizione	Redatto	Verificato	Approvato
0	**24/05/2018**	**Emissione**	**DR. LUIGI PUCINO**	**DR. LUIGI PUCINO**	**DR. LUIGI PUCINO**

Capitolo 2
RUOLI, COMPITI E NOMINA DELLE FIGURE PER LA SICUREZZA

2.1 Titolare del Trattamento

Il **Titolare del trattamento** è 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;
Articolo 24
Responsabilità del titolare del trattamento

1) Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2) Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3) L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Il **Titolare del trattamento** deve assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del GDPR tese a ridurre al minimo il rischio di distruzione e perdita dei dati personali, accessi non autorizzati o trattamenti non consentiti.
Il **Titolare del Trattamento** mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili del trattamento** che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del GDPR. Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile del Trattamento**, ne assumerà tutte le responsabilità e funzioni.

2.2 Responsabile del Trattamento

2.2.1 Ruolo del Responsabile del Trattamento

Articolo 28
Responsabile del Trattamento

1) Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
2) Il responsabile del trattamento non ricorre a un altro responsabile senza previa **autorizzazione scritta**, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3) I trattamenti da parte di un responsabile del trattamento sono **disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri**, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la **materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento**

Il **Titolare del Trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto uno o più **Responsabili del Trattamento** con il compito di individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Incaricati del trattamento**. Qualora il **Responsabile del Trattamento** ritenga di non nominare alcun **Incaricato di uno specifico trattamento**, ne assumerà tutte le responsabilità e funzioni.

La nomina del responsabile del trattamento è, quindi, discrezionale, ma se il **titolare del trattamento** si avvale di soggetti esterni deve nominarli **responsabili del trattamento.** Le mansioni dei Responsabili del Trattamento esterni sono descritte al punto 3.8 di questo registro.

Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il **Titolare del trattamento** dovrebbe ricorrere unicamente a **Responsabili del Trattamento** che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento.

L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata da un **contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri che vincoli il **Responsabile del Trattamento** al **Titolare del Trattamento**, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato.

Dopo il completamento del trattamento per conto del **Titolare del Trattamento**, il **Responsabile del Trattamento** dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali.

Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile del Trattamento**, ne assumerà tutte le responsabilità e funzioni.

2.2.2 Nomina dei Responsabili del Trattamento

La nomina di ciascun **Responsabile del Trattamento** deve essere effettuata dal **Titolare del trattamento** con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione. Le specifiche per la nomina del Responsabile del trattamento sono definite in accordo con l'art.28 comma 3 del GDPR.
Il **contratto o altro atto giuridico per la nomina del Responsabile del Trattamento** prevede, in particolare, che il responsabile del trattamento:

a. tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b. garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c. adotti tutte le misure richieste ai sensi dell'articolo 32;
d. rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e. tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f. assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g. su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h. metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo

alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Copia del contratto per la nomina accettata deve essere conservata a cura del **Titolare del trattamento** in luogo sicuro.

Il **Titolare del trattamento** deve informare ciascun **Responsabile del Trattamento** delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal GDPR.

Il **Titolare del trattamento** deve consegnare a ciascun **Responsabile del Trattamento** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del **Responsabile del Trattamento** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del **Responsabile del Trattamento** può essere revocata in qualsiasi momento dal **Titolare del trattamento** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

2.3 Incaricato del trattamento

Gli **Incaricati del trattamento** sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali **dal titolare del trattamento**.

La nomina di ciascun **Incaricato del trattamento dei dati personali** deve essere effettuata dal **Titolare del trattamento.**
.
Il **Titolare del trattamento** deve informare ciascun **Incaricato del trattamento dei dati personali** delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal GDPR.

Il **Titolare del trattamento** deve consegnare a ciascun **Incaricato del trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

Gli **Incaricati del trattamento dei dati personali sensibili** devono ricevere idonee ed analitiche **istruzioni scritte**, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

La nomina dell'**Incaricato del trattamento dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'**Incaricato del trattamento dei dati personali** può essere revocata in qualsiasi momento dal **Titolare del trattamento** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

Capitolo 3
ELENCO DEI TRATTAMENTI DEI DATI

3.1 Periodicità di revisione del Registro del Trattamento

Il **Titolare del trattamento** deve effettuare una revisione periodica del **Registro del** Trattamento, con frequenza almeno annuale, ed eventualmente predisporre una nuova versione del **Registro del Trattamento** contenente idonee informazioni riguardo all'articolo 30 del GDPR in caso di revisioni da parte della Commissione Europea o in caso di adeguamenti legislativi apportati dal **Garante della Privacy** italiano.

3.2 Elenco dei trattamenti di dati personali

Il **Titolare del Trattamento**, in collaborazione con i **Responsabili del Trattamento,** redige un "elenco dei trattamenti", che costituisce una mappatura di tutte le aree e processi in cui sono presenti i dati personali con cui DR. LUIGI PUCINO entra in contatto. L'elenco dei trattamenti è costituito dall'allegato nel quale è ricavabile quanto segue:

3.2.1 Elenco delle sedi e degli uffici in cui vengono trattati i dati

Al **Titolare del Trattamento** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.

l'Elenco delle sedi in cui vengono trattati i dati deve essere aggiornato e conservato in luogo sicuro a cura del **Titolare del Trattamento**.

3.2.2 Elenco degli archivi dei dati oggetto del trattamento

Al **Titolare del Trattamento** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.
Ogni **banca di dati** o archivio deve essere classificato in relazione alle informazioni contenute indicando se si tratta di:

- Dati personali Comuni
- Dati personali Sensibili (Biometrici, Relativi alla Salute, Relativi a Opinioni Politiche, Relativi all'orientamento e alla vita sessuale dell'individuo)
- Dati personali Giudiziari

3.2.3 Elenco dei sistemi di elaborazione per il trattamento

Al **Titolare del Trattamento** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

3.3 Distribuzione compiti e responsabilità nell'ambito delle strutture preposte al trattamento dei dati

3.3.1 Elenco dei soggetti autorizzati al trattamento dei dati

Il **Titolare del Trattamento** di aggiornare l'**elenco del personale autorizzato al trattamento dei dati** che deve essere conservato a cura del **Titolare del Trattamento**, in luogo sicuro. Vedere Nomine Soggetti Autorizzati.

3.3.2 Formazione dei soggetti autorizzati al trattamento dei dati

Il **Titolare del trattamento dei dati personali** valuta, per ogni incaricato a cui ha affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.

La previsione di interventi formativi degli incaricati del trattamento, ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Al **Titolare del Trattamento** è affidato il compito di verificare ogni anno le necessità di ulteriore formazione del personale incaricato di effettuare periodicamente le operazioni di copia di sicurezza delle banche di dati trattate.

3.4 Analisi dei rischi che incombono sui dati

3.4.1 Manutenzione dei sistemi di elaborazione dei dati

Il **Titolare**, anche avvalendosi di consulenti interni o esterni, deve di verificare ogni anno:

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito

Il **Titolare** deve redigere ogni anno il **Report annuale dei rischi e il Piano di trattamento dei rischi**.

Nel caso in cui esistano rischi evidenti il **Titolare del Trattamento** deve adottare gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.4.2 Manutenzione dei sistemi operativi e dei software installati

Al **Titolare** è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei software utilizzati.
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Nel cui esistano rischi evidenti il **Titolare del Trattamento** deve adottare gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.4.3 Gestione del Rischio

L'analisi dei rischi non è stata condotta in quanto non si ritiene necessaria non trattando dati particolari.

3.5 Misure da adottare per garantire l'integrità e la disponibilità dei dati

Il **Titolare dei trattamenti** al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banca di dati da lui trattati.
I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Al **Titolare del Trattamento** è affidato il compito di verificare ogni anno, le necessità di formazione del personale incaricato di effettuare periodicamente le Copie di sicurezza delle banche di dati trattate, in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica.

3.6 Misure di sicurezza tecniche e organizzative

3.6.1 Misure generali

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** mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il **Titolare del Trattamento** fà sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti 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.

3.6.2 Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Al **Titolare del Trattamento** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, e di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il **Titolare del Trattamento** deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

3.7 Notifica di una violazione dei dati personali all'autorità di controllo e ai diretti interessati

3.7.1 Notifica all'autorità

In caso di violazione dei dati personali, il **Titolare del Trattamento** notifica la violazione all'**autorità di controllo competente** entro 72 ore dal momento in cui ne è venuto a conoscenza.

Qualora la notifica all'**autorità di controllo** non sia effettuata entro 72 ore, saranno esposti i motivi del ritardo.

il **Titolare del Trattamento** senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica:

- descrive la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunica il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrive le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del **Titolare del trattamento** per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il **Titolare del trattamento** documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Le violazioni dei dati personali, se presenti, sono raccolte nel **Registro Violazioni dati Personali**.

3.7.2 Notifica all'interessato

Quando la violazione dei dati personali potrebbe presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il **Titolare del Trattamento** comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive la natura della violazione dei dati personali:

- comunica il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrive le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte del **Titolare del trattamento** per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

3.8 Dati personali affidati all'esterno della struttura del titolare

3.8.1 Trattamenti di dati personali affidati all'esterno della struttura del titolare

Il **Titolare del Trattamento**, può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura.

Il **Titolare del Trattamento**, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

- I soggetti interessati
- I luoghi dove fisicamente avviene il trattamento dei dati stessi
- I responsabili del trattamento di dati personali

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, che deve essere conservato a cura del **Titolare del Trattamento**, in luogo sicuro.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, sia possibile nominare responsabili del trattamento soggetti controllabili dal **Titolare del trattamento** stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso).

3.8.2 Nomina del responsabile del trattamento esterno

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il **Titolare del Trattamento** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno, per questo si avvale della nomina di un **Responsabile del Trattamento,** secondo i criteri descritti dal capitolo 2.2 di questo registro.

La nomina del **Responsabile del trattamento** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Titolare del Trattamento** in luogo sicuro.

3.9 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

3.9.1 Protezione contro l'accesso abusivo

Al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il **Titolare del Trattamento**, stabilisce le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.

I criteri debbono essere definiti dal **Titolare del Trattamento** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- Le misure applicate per evitare intrusioni.
- Le misure applicate per evitare contagi da "Virus Informatici".

3.9.2 Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Il **Titolare del Trattamento** è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati.

Per ogni banca di dati deve essere individuato il luogo di conservazione copie dei dati in modo che sia convenientemente protetto dai potenziali rischi di:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto

3.9.3 Riutilizzo dei supporti rimovibili

Se il **Titolare del Trattamento** decide che i supporti magnetici contenenti dati sensibili o giudiziari non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.

È compito del **Titolare del Trattamento** assicurarsi che in nessun caso vengano lasciate copie di **Banche di dati** contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

3.9.4 Ripristino dell'accesso ai dati in caso di danneggiamento

La decisione di rispristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del **Titolare del Trattamento**.

La decisione di rispristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro sette giorni.

Una volta valutata la assoluta necessità di rispristinare la disponibilità dei dati in seguito a distruzione o danneggiamento il **Titolare del Trattamento** deve provvedere tramite l'**Incaricato delle copie di sicurezza delle banche dati** e tramite **il Responsabile della gestione e della manutenzione degli strumenti elettronici** all'operazione di ripristino dei dati.

La decisione di rispristinare la funzionalità degli elaboratori elettronici guasti deve essere presa rapidamente e in ogni caso la funzionalità deve essere ripristinata al massimo entro sette giorni.

3.9.5 Trattamento effettuato da organismi sanitari e esercenti le professioni sanitarie

Il **Titolare del Trattamento** deve assicurare che nel caso in cui siano presenti banche dati contenenti dati personali idonei a rivelare lo stato di salute e la vita sessuale vengano adottate le seguenti misure:

- Garantire in ogni momento l'impossibilità dell'accesso non autorizzato all'infrastruttura ed ai supporti di dati.
- Escludere l'accesso di persone non autorizzate a dati personali utilizzando un sistema di controllo delle credenziali di autenticazione.
- Che le informazioni, se trasmesse siano cifrate e che la cifratura rispetti un livello tecnico adeguato all'attuale stato dell'arte.
- Che l'identificazione dell'utente interessato che ha il diritto di ricevere i dati deve essere garantita in modo univoco.
- Per tutti i servizi tramite Internet il sistema di sicurezza deve essere basato su un protocollo TCP/IP con crittografia Secure Socket Layer (SSL) a 128 bit strong encryption emesso da Verisign Certification Authority per dare la massima garanzia che le informazioni che transitano sulla rete siano visibili unicamente dall'utente interessato. L'utilizzo di una chiave di cifratura a 128 bit garantisce il massimo livello di sicurezza a protezione del mutuo scambio di informazioni con l'utente interessato. Il tempo necessario per decodificare tale chiave è infatti virtualmente infinito (circa $3 \cdot 10^{38}$ possibili combinazioni).
- Deve essere garantita la separazione architetturale tra le macchine contenenti i dati personali idonei a rivelare lo stato di salute e la vita sessuale e i server collegati ad Internet.

3.10 Misure di tutela e garanzia

3.10.1 Descrizione degli interventi effettuati da soggetti esterni

Nel caso in cui ci si avvale di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento hardware e/o software degli strumenti elettronici e alla eventuale riparazione, aggiornamento o sostituzione, il **Titolare del Trattamento**, deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità.

Capitolo 4
FINALITÀ DEL TRATTAMENTO

4.1 Categorie di interessati e categorie di dati degli interessati

DR. LUIGI PUCINO tratta dati dei clienti e dei fornitori e dei loro referenti e dei propri dipendenti come meglio specificato nell'allegato al REGISTRO DEI TRATTAMENTI. Inoltre tratta dati sanitari dei propri pazienti e dei lavoratori in merito alla medicina del lavoro.

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato seguendo i principi descritti dal GDPR art. 5,6 di:
liceità;
correttezza;
trasparenza;
I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; Il **Titolare del Trattamento** si accerta che i dati personali siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); Questi principi, che corrispondono con i diritti dell'interessato sono meglio descritti nel capitolo 5 del presente Registro del Trattamento.

Il Titolare del Trattamento DR. LUIGI PUCINO tratta i dati personali solo se soddisfano almeno una delle seguenti condizioni in accordo con l'articolo 6 del GDPR:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il **Titolare del Trattamento** ;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per il perseguimento del legittimo interesse del **Titolare del Trattamento** o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il **Titolare del Trattamento** tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra **l'interessato** e il **Titolare del Trattamento**;
c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali sensibili (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) oppure se siano trattati dati relativi a condanne penali e a reati;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Capitolo 5
DIRITTI DELL'INTERESSATO

5.1 Trasparenza e modalità

Il **Titolare del Trattamento** adotta misure appropriate per fornire all'interessato tutte le informazioni in possesso dell'azienda e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Il **Titolare del Trattamento** agevola l'esercizio dei diritti dell'interessato riportati negli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il **Titolare del Trattamento** non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

Il **Titolare del Trattamento** fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

Se non ottempera alla richiesta dell'interessato, il **Titolare del Trattamento** informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale. La proroga può estendersi fino

al secondo mese dal momento della richiesta dell'interessato.

Le informazioni fornite all'interessato sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il **Titolare Del Trattamento** può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure
b) rifiutare di soddisfare la richiesta.

Incombe al **Titolare Del Trattamento** l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Nel caso in cui il **Titolare del Trattamento** non sia sicuro dell'identità di chi sta chiedendo i dati personali, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

5.2 Informazione e accesso ai dati personali

5.2.1 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

In caso di raccolta presso l'interessato di dati che lo riguardano, il **Titolare del Trattamento** fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del **Titolare del Trattamento** e, ove applicabile, del suo **rappresentante**;
b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
c) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal **Titolare del Trattamento** o da terzi;
d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e) ove applicabile, l'intenzione del **Titolare del Trattamento** di trasferire dati personali a un **paese terzo** o a **un'organizzazione internazionale** e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

In aggiunta alle informazioni precedenti, nel momento in cui i dati personali sono ottenuti, il **Titolare del Trattamento** fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al **Titolare del Trattamento** l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sul consenso fornito al **Titolare del Trattamento** (articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a)), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, in tali casi, vengono fornite all'interessato informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora il **Titolare del Trattamento** intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

5.2.2 Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

Qualora i dati non siano stati ottenuti presso l'interessato, il **Titolare del Trattamento** fornisce all'interessato le seguenti informazioni:

a) l'identità e i dati di contatto del **Titolare del Trattamento** e, ove applicabile, del suo rappresentante;
b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
c) le categorie di dati personali in questione;

d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
e) ove applicabile, l'intenzione del **Titolare del Trattamento** di trasferire dati personali a un **paese terzo** o a **un'organizzazione internazionale** e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili

Il **Titolare del Trattamento** fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal **Titolare del Trattamento** o da terzi;
c) l'esistenza del diritto dell'interessato di chiedere al **Titolare del Trattamento** l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia basato sul consenso fornito al **Titolare del Trattamento** (articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a)), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
g) l'esistenza di un processo decisionale automatizzato, in tali casi, vengono fornite all'interessato informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il **Titolare del Trattamento** fornisce le informazioni precedentemente elencate:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati.

Qualora il **Titolare del Trattamento** intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

I punti precedentemente elencati non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato. In tali casi, il **Titolare del Trattamento** adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato;
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

5.2.3 Diritto di accesso dell'interessato

L'interessato ha il diritto di ottenere dal **Titolare del Trattamento** la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al **Titolare del Trattamento** la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o

di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, **l'interessato** ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il **Titolare del Trattamento** può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia dei dati personali dell'interessato non deve ledere i diritti e le libertà altrui.

5.3 Rettifica e cancellazione

5.3.1 Diritto di rettifica

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

5.3.2 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 conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 (paragrafo 5.4.1 del Registro del Trattamento), e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i **Titolari del Trattamento** che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I punti precedentemente annunciati nel paragrafo non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;
b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il **Titolare del Trattamento**;
c) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

5.3.3 Diritto alla limitazione del trattamento

L'interessato ha il diritto di ottenere dal **Titolare del Trattamento** la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al **Titolare del Trattamento** per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il **Titolare del Trattamento** non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del GDPR (paragrafo 5.4.1 del Registro del Trattamento), in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma di quanto appena citato nel presente paragrafo, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'interessato che ha ottenuto la limitazione del trattamento è informato dal **Titolare del Trattamento** prima che detta limitazione sia revocata.

5.3.4 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il **Titolare del Trattamento** comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dei paragrafi 5.3.1, 5.3.2, 5.3.3 del presente Registro dei Trattamenti, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il **Titolare del Trattamento** comunica all'interessato tali destinatari qualora l'interessato lo richieda.

5.3.5 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 (ai sensi dell'articolo 6, paragrafo 1, lettera a) , o dell'articolo 9, paragrafo 2, lettera a) del GDPR), o su un contratto (ai sensi dell'articolo 6, paragrafo 1, lettera b) del GDPR); e
b) il trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma di quanto appena descritto, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un **Titolare del Trattamento** all'altro, se tecnicamente fattibile.

Il diritto alla portabilità dei dati non deve ledere i diritti e le libertà altrui.

5.4 Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

5.4.1 Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettera f) (il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali) compresa la profilazione sulla base di tali disposizioni.

Il **Titolare del Trattamento** si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

Il diritto di opposizione è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

5.4.2 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Quanto appena annunciato non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un **Titolare del Trattamento**;
b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) si basi sul consenso esplicito dell'interessato.

Nei casi di cui i precedenti punti a) e c), il **Titolare del Trattamento** attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del **Titolare del Trattamento**, di esprimere la propria opinione e di contestare la decisione.

Le decisioni elencate nell'elenco puntato precedentemente esposto non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 (È vietato trattare 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,) a meno che non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato o non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g)

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

Capitolo 6
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

TRATTAMENTO CON STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in

possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Registro del Trattamento

19. Ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un Registro del Trattamento contenente idonee informazioni riguardo:

a. l'elenco dei trattamenti di dati personali;
b. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
c. l'analisi dei rischi che incombono sui dati;
d. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
e. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
f. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
g. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, all'esterno della struttura del titolare;
h. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.
21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.
24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.
26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del Registro del Trattamento.

TRATTAMENTO SENZA L'AUSILIO DI MEZZI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

1. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche

per classi omogenee di incarico e dei relativi profili di autorizzazione.

2. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
3. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Capitolo 7
PROCEDURE

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

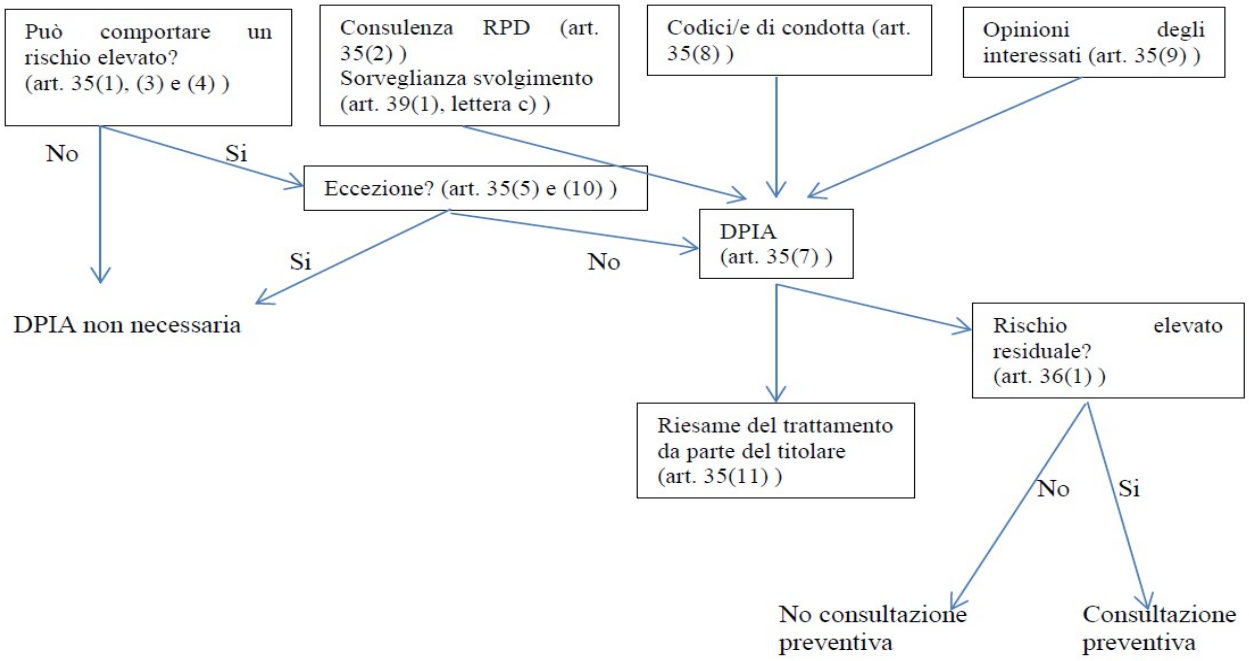
Il **Titolare del Trattamento** di DR. LUIGI PUCINO non effettua, come descritto al paragrafo 3.4.3 una valutazione del rischio sui processi che possono comportare un rischio per i diritti e le libertà degli interessati.

Il **Titolare del Trattamento** valuta inoltre se effettuare o meno una valutazione di impatto sulla protezione dei dati (Data Protection Impact Assessment, DPIA) seguendo la linea guida proposta dal Garante per la Protezione dei Dati Personali Italiano (17 EN WP 248) prendendo in esame i seguenti nove criteri:

1) Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive
2) Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura
3) Monitoraggio sistematico
4) Dati sensibili o dati di natura estremamente personale
5) Trattamenti di dati su larga scala
6) Combinazione o raffronto di insiemi di dati
7) Dati relativi a interessati vulnerabili (considerando 75
8) Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
9) Tutti quei trattamenti che, di per sé, “impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto” (art. 22 e considerando 91).

Il **Titolare del Trattamento** può ritenere, che quando un trattamento soddisfa almeno due dei criteri sopra indicati sia necessario condurre una DPIA.

In caso si presentasse la necessità di svolgere una valutazione di impatto sulla protezione dei dati, la DPIA di DR. LUIGI PUCINO segue il flusso descritto dal Garante per la Protezione dei Dati Personali Italiano (17 EN WP 248).



INDICE DEGLI ARGOMENTI

Allegati

Descrizione
Registro dei Trattamenti
Nomina responsabili esterni al trattamento
Informative e Consensi