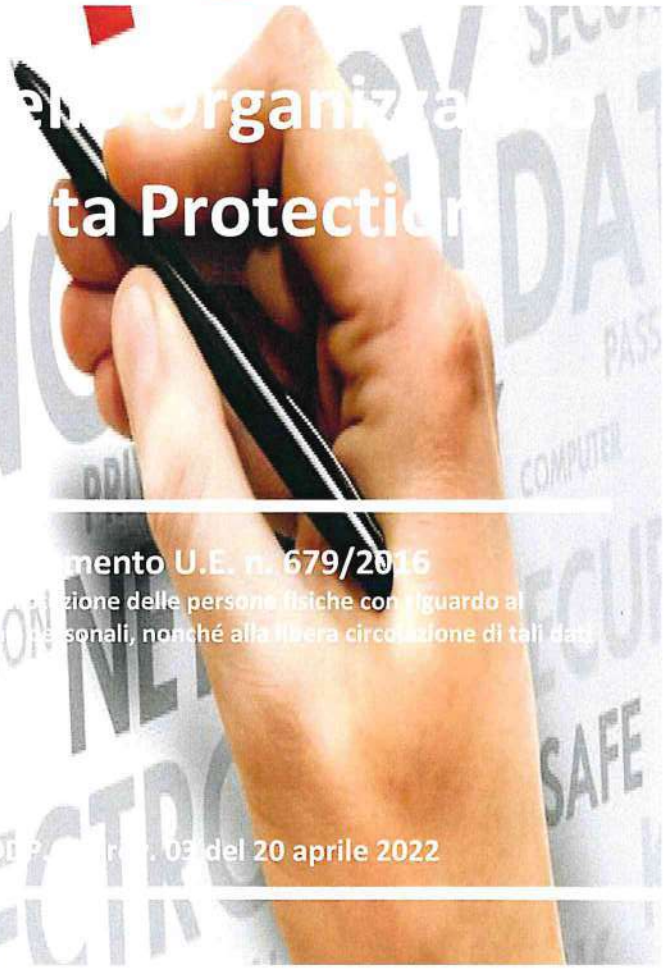
SISIFO
CONSORZIO
DI COOPERATIVE
SOCIALI

PRIVACY

Modello Organizzativo
Data Protection



Regolamento U.E. n. 679/2016
relativo alla protezione delle persone fisiche con riguardo al
trattamento dei dati personali, nonché alla libera circolazione di tali dati

MOD Privacy n. 03 del 20 aprile 2022

STATO DEL DOCUMENTO: LISTA DELLE REVISIONI

REV. N.	DATA	DESCRIZIONE
03	20.04.2022	Terza emissione

DOCUMENTO	REDAZIONE	VERIFICA	AUTORIZZAZIONE
DOC: MODP.679 REV.: 03 DATA: 20.04.2022	Firma SISIFO CONSORZIO COOPERATIVE SOCIALI Il Presidente Piccolo Giuseppe (Titolare del Trattamento)	Firma (Referente GDPR)	Firma SIAPA Soluzioni Integrate per l'Azienda e la P.A. (Responsabile Protezione Dei Personali) (Responsabile Protezione dei Dati)

Sommario

1. DEFINIZIONI

Questo documento descrive il Modello Organizzativo Data Protection predisposto al fine di ottemperare a quanto prescritto dal Regolamento UE n. 679/2016 in materia di protezione dei dati personali e adottato da **SISIFO Consorzio di Cooperative Sociali a r.l.**

Appare preliminarmente opportuno fornire una serie di definizioni utili alla migliore comprensione del Modello.

Regolamento o GDPR	Il Regolamento UE n. 679/2016 sulla protezione dei dati personali, adottato il 27 aprile 2016 dal Parlamento Europeo e dal Consiglio, con entrata in vigore a partire dal 25 maggio 2018.
Modello Organizzativo o Modello o MODP	Modello Organizzativo Data Protection adottato dall'Organizzazione che raccoglie in sé una mappatura dei dati trattati, l'analisi dei rischi e degli impatti e le misure tecniche e organizzative, ivi incluse le procedure organizzative e gestionali, adottate per prevenire i suddetti rischi.
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.
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.
Limitazione di trattamento	Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
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.
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.
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.
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.
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.
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.
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.
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.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati 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.
Stabilimento principale	a) 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; b) 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 GDPR.
Rappresentante	La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile el trattamento per iscritto ai sensi dell'art. 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del GDPR.
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.
Gruppo imprenditoriale	Un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.
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.
Autorità di controllo	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR. Per l'Italia, detta autorità è individuata nel Garante per la protezione dei dati personali.
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; c) un reclamo è stato proposto a tale autorità di controllo.
Trattamento transfrontaliero	a) 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; b) 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.
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 GDPR, 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.
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.
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.
Responsabile della protezione dei dati (RPD-DPO)	Soggetto nominato obbligatoriamente nei casi previsti dall'art. 37 del GDPR o facoltativamente, con i seguenti compiti: • sorvegliare l'osservanza del GDPR, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità; • collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA); • informare e sensibilizzare il titolare/responsabile nonché i di loro dipendenti riguardo gli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati; • cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento; • supportare il titolare/responsabile in ogni attività connessa al trattamento dei dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento

2. IL QUADRO NORMATIVO

2.1. Introduzione

Il Regolamento UE n. 679/2016 sulla protezione dei dati personali (di seguito denominato "GDPR"), abrogativo della precedente Direttiva n. 95/46/CE, è entrato in vigore il 24 maggio 2016 con applicazione rinviata al 25 maggio 2018.

L'introduzione del GDPR cambia in maniera sostanziale l'approccio che si è avuto sinora sulla privacy: d'ora in avanti il quadro normativo sarà incentrato sui doveri e sulla responsabilizzazione del Titolare del trattamento, secondo il principio della "accountability".

La nuova disciplina impone al Titolare del trattamento di garantire il rispetto dei principi contenuti nel GDPR, ma anche la capacità di comprovare di aver adottato le misure tecniche e organizzative idonee a prevenire il verificarsi dei rischi.

In particolar modo il concetto di "responsabilizzazione" si traduce nel fatto che il Titolare è chiamato a dimostrare che i trattamenti siano coerenti con il disposto del GDPR, a pianificare e mettere in atto misure tecniche e organizzative per poterne comprovare l'adeguatezza, e ad attivare un modello di monitoraggio delle misure tecnico-organizzative implementate.

In un contesto, quale quello sanitario, nel quale si trattando tipologie di dati particolari relativi allo stato di salute, la necessità di adottare misure tecniche e organizzative vieppiù idonee diviene ancor più essenziale.

2.2. Definizione di trattamento

L'art. 4 del GDPR definisce il trattamento dei dati personali come 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.

Di seguito vengono riassunte alcune delle principali operazioni che possono configurare trattamento ai sensi dell'art. 4 del GDPR:

- raccolta: consiste nell'acquisizione delle informazioni, in qualunque modo essa avvenga (ad esempio direttamente dalla persona interessata o presso terzi)
- registrazione: consiste nella memorizzazione dei dati su un qualsiasi supporto;
- organizzazione: consiste nella classificazione dei dati secondo un metodo prescelto;
- strutturazione: consiste nell'attività di distribuzione dei dati secondi schemi precisi;
- conservazione: consiste nel mantenere memorizzate le informazioni su un qualsiasi supporto;
- consultazione: è la mera lettura dei dati personali. Anche la mera visualizzazione dei dati è un trattamento che può rientrare nell'operazione di consultazione;
- elaborazione: consiste nell'attività con la quale il dato personale subisce una modifica sostanziale. La modificazione differisce dall'elaborazione in quanto può riguardare anche solo parte minima del dato personale;
- selezione: consiste nell'individuazione di dati personali nell'ambito di gruppi di dati già memorizzati;
- estrazione: consiste nell'attività di estrapolazione di dati da gruppi già memorizzati;
- raffronto: è un'operazione di confronto tra dati, sia una conseguenza di elaborazione che di selezione o consultazione;
- utilizzo: è un'attività generica che ricopre qualsiasi tipo di impiego dei dati;
- interconnessione: consiste nell'utilizzo di più banche dati, e si riferisce all'impiego di strumenti elettronici;
- blocco: consiste nella conservazione con sospensione temporanea di ogni altra operazione di trattamento;
- comunicazione (o cessione): consiste nel dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal responsabile e dagli incaricati. Si tratta di un'operazione delicata perché i dati vengono comunicati a terzi;
- diffusione: consiste nel dare conoscenza dei dati a soggetti indeterminati, in qualunque forma anche mediante la loro messa a disposizione o consultazione;

- limitazione: consiste nel contrassegnare dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- cancellazione: consiste nell'eliminazione di dati tramite utilizzo di strumenti elettronici;
- distruzione: è l'attività di eliminazione definitiva dei dati.

2.3. Principi applicabili al trattamento di dati personali

L'art. 5 del GDPR elenca i principi applicabili al trattamento di dati personali, riassunti nella successiva tabella:

PRINCIPIO	DESCRIZIONE
Principio di liceità	I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
Principio di finalità	I dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali.
Principio di minimizzazione dei dati	I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
Principio di esattezza	I dati personali sono esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
Principio di conservazione	I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato.
Principio di integrità e riservatezza	I dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Corollario di detti principi è quello della "responsabilizzazione" del titolare del trattamento, il quale deve non solo mettere in atto misure tecniche e organizzative atte a consentire il rispetto dei suddetti principi, ma anche essere in grado di comprovarlo.

2.3.1. Principio di liceità

Ogni trattamento deve trovare fondamento in un'idonea base giuridica. L'articolo 6 del GDPR identifica i casi in cui il trattamento è da considerarsi lecito:

- in caso di consenso dell'interessato al trattamento dei dati per una specifica finalità. In caso di dati sensibili o per le decisioni basate su trattamenti automatizzati - inclusa la profilazione - il consenso deve essere esplicito;
- se il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dell'interessato;
- se il trattamento è necessario per l'adempimento di obblighi derivanti da legge, regolamento o normativa dell'Unione o dello Stato membro cui è soggetto il titolare;
- se il trattamento è necessario per la salvaguardia di interessi vitali dell'interessato o di un'altra persona fisica;
- se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- se il trattamento è necessario per il perseguimento di legittimi interessi 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.

2.3.2. Principio di finalità

Il trattamento di dati personali presuppone una finalità determinata, esplicita e legittima e modalità di utilizzo compatibili con tale finalità.

Di conseguenza, ogni finalità sorta in un momento successivo alla raccolta dei dati necessita di una nuova informativa.

Questa circostanza si verifica con frequenza nei trattamenti che utilizzano le più moderne tecnologie. In questi casi si parla della c.d. function creep (in italiano, estensione indebita delle funzionalità), ossia il caso in cui sorgono nuove finalità sulla base di particolari tipi di dati e di strumenti tecnologici utilizzati dal Titolare per trattare i dati stessi.

A differenza del Codice Privacy che utilizzava il termine "manifesta", il GDPR si riferisce a una finalità "esplicita". Si ritiene che la differenza sia lessicale, ma non sostanziale. Infatti, entrambi i concetti sono diretta declinazione del principio di trasparenza, che è alla base sia del GDPR sia del Codice Privacy.

L'obiettivo è assicurare la consapevolezza del trattamento all'interessato.

2.3.3. Principio di minimizzazione dei dati

Questo principio è inerente al rapporto tra dati e trattamento. I dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

In questo principio si possono includere quelli che il Codice Privacy definiva principi di pertinenza, necessità e non eccedenza. La pertinenza indica la rilevanza che l'informazione assume in relazione alla finalità del trattamento. Inoltre, i dati raccolti devono essere sufficienti ai fini del trattamento, ma non eccedenti.

Pertanto, la natura e la quantità di dati personali raccolti saranno adeguate quando saranno essenziali e funzionali al trattamento stesso.

Il concetto di non eccedenza può essere rispettato in concreto tramite verifiche periodiche atte ad accertare che la conservazione dei dati sia in linea con le finalità del trattamento.

2.3.4. Principio di esattezza

Quando il dato raccolto è inesatto, il trattamento non è lecito. Ciò impone al Titolare di verificare periodicamente l'attendibilità dei dati personali, anche senza un'espressa richiesta dell'Interessato o del Garante. Di conseguenza, il dato deve essere esatto e, quando necessario, aggiornato.

Il Titolare deve:

- adottare le misure necessarie per rettificare o eliminare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati e
- verificare la correttezza del dato raccolto con quelli inerenti allo stesso interessato ma raccolti in momenti diversi o che abbiano diversa provenienza.

L'illiceità del trattamento è ancora più grave quando il dato inesatto è invariante (si pensi, ad esempio, al nome o alla data di nascita dell'interessato o a tutti quelli biometrici).

Il dato inesatto potrebbe anche non essere errato, ma semplicemente incompleto. Per questa ragione l'art. 16 del GDPR prevede la possibilità per l'interessato di chiedere e ottenere senza ingiustificato ritardo la rettifica o l'integrazione dei propri dati personali nella disponibilità del titolare.

2.3.5. Principio di conservazione

I dati raccolti devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

D'altro canto, un periodo di conservazione eccessivo impedisce all'Interessato (ma anche al Titolare) di vigilare sul trattamento. Inoltre, aumenta il rischio che il dato personale venga danneggiato, distrutto oppure trattato da un soggetto non autorizzato.

Per evitare di conservare un dato personale troppo a lungo, il Titolare potrà adottare procedure periodiche atte ad accertare la necessità di conservare o meno i dati nella sua disponibilità in relazione ai fini del trattamento.

In ogni caso, i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

2.3.6. Principio di integrità e riservatezza

Il titolare deve garantire adeguata sicurezza e protezione dei dati trattati mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

La valutazione dell'adeguatezza del livello di sicurezza è basata sui rischi presentati dal trattamento che derivano:

- dalla distruzione;
- dalla perdita;
- dalla modifica;
- dalla divulgazione non autorizzata;
- dall'accesso in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

2.4. Trattamento di categorie particolari di dati personali

L'art. 9 del GDPR detta regole specifiche per alcune particolari categorie di dati personali, di seguito elencate:

- dati genetici;
- dati biometrici;
- dati relativi alla salute;
- dati idonei a rivelare:
  - l'origine razziale o etnica;
  - le opinioni politiche;
  - le convinzioni religiose o filosofiche;
  - l'appartenenza sindacale;
  - la vita sessuale o l'orientamento sessuale.

I suddetti dati corrispondono pressoché integralmente a quelli che, in vigenza del Codice Privacy, venivano identificati come "dati sensibili".

I suddetti dati possono essere trattati esclusivamente se:

- l'interessato è ha prestato il proprio consenso;
- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento è necessario per motivi di interesse pubblico rilevante;

- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica;
- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

2.4.1. Dati relativi alla salute

Il GDPR sottolinea che proprio per la peculiarità e la delicatezza che contraddistingue i dati relativi alla salute (cartelle cliniche, stato di salute, trattamenti sanitari, terapie, analisi del corredo genetico, ecc.), nell'ipotesi in cui questi dovessero essere utilizzati per:

- finalità di medicina preventiva (ad es. villocentesi e amniocentesi se correlate ad informazioni genetiche) o di medicina del lavoro;
- la valutazione della capacità lavorativa del dipendente;
- diagnosi, assistenza o terapia sanitaria o sociale;
- gestione dei sistemi e servizi sanitari o sociali

questi debbano essere trattati da soggetti che siano autorizzati dalla normativa nazionale o iscritti in appositi albi professionali per i quali, solitamente, vengono previsti precisi oneri e doveri deontologici che possano assicurare il rispetto delle libertà e dei diritti dell'interessato (ad es. i medici).

2.4.2. Dati che rivelano l'origine razziale o etnica

Nella pratica, questo tipo di informazioni, possono essere rivelate attraverso documenti identificativi che, solitamente, indicano esplicitamente il paese di provenienza del soggetto a cui fanno riferimento ed il cui trattamento è consentito se ricade nelle ipotesi di cui sopra.

Il trattamento dei dati in oggetto può verificarsi nella prassi:

- nei casi di assunzione di lavoratori (es. i dati anagrafici del lavoratore a fini previdenziali e, in alcuni casi, anche solo il nome e il cognome del lavoratore possono rivelare l'origine razziale o etnica);
- nei casi di accertamento che scaturiscono dall'esercizio o dalla difesa di un diritto in sede giudiziaria (es. i dati identificativi della parte nell'ambito di un processo, in fase di indagine o per la redazione degli atti);
- nelle ipotesi in cui l'interessato dovesse essere sottoposto ad un'operazione chirurgica (es. per redigere la cartella clinica);
- nelle attività che possono essere svolte da parte di associazioni umanitarie senza scopo di lucro che cercano di assistere i soggetti anche in ragione alle difficoltà scaturite dalla provenienza da un determinato paese (es. fondazioni umanitarie che aiutano l'integrazione degli stranieri, all'interno del nostro paese, proponendo iniziative e progetti multiculturali).

2.4.3. Dati concernenti le opinioni politiche

Un'altra delle categorie particolari, di dati personali, che viene presa in considerazione è quella che permette di rivelare le opinioni politiche dell'interessato, i cui dati sono oggetto del trattamento. In questa ipotesi, uno degli esempi pratici, potrebbe essere quello delle tessere di iscrizione ad un determinato partito politico (ad es. in sede di adesione ad attività promosse dalle, o presso le, segreterie politiche).

2.4.4. Dati riguardanti le convinzioni religiose o filosofiche

I dati idonei a rivelare convinzioni religiose o filosofiche, nella pratica, sono trattati in particolari situazioni. Ad esempio, in relazione alla necessità di dover compiere un determinato tipo di intervento o terapia, nel rispetto degli obblighi imposti dalla legge in merito ai trattamenti sanitari (v. art. 32 Costituzione e art. 54 c.p.), può essere utile se non addirittura necessario, conoscere il credo religioso del paziente poiché potrebbe, egli stesso, negare il proprio consenso a sottoporsi a determinate pratiche terapeutiche (es. i membri della Chiesa dei testimoni di Geova rifiutano, secondo i loro principi religiosi, le emotrasfusioni di sangue). Anche nell'ambito del rapporto di lavoro subordinato, trattare dati relativi alle convinzioni religiose del dipendente potrebbe essere necessario per gestire le assenze del lavoratore in corrispondenza con le festività previste da una determinata religione.

2.4.5. Dati sull'appartenenza sindacale

Un'altra categoria particolare di dati personali che viene presa in considerazione da parte del legislatore Europeo, all'interno del GDPR, è quella che permette di individuare l'appartenenza sindacale dell'interessato. L'esempio tipico è quello dell'ufficio della contabilità, di un'azienda o di una società, che nell'ambito dell'emissione delle retribuzioni, all'interno della documentazione riguardante gli stipendi (i c.d. cedolini) indica, tra le ritenute, quelle disposte in favore del corrispondente gruppo sindacale secondo quanto indicato dall'interessato.

2.4.6. Dati biometrici

Essi rappresentano i dati personali ottenuti da un trattamento tecnico specifico relativo 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 (impronte digitali). Una delle cause di legittimità, esplicitamente previste all'interno dell'art. 9 del GDPR, è quella che richiama il diritto dell'Unione o degli Stati membri oltre alle ipotesi di esercizio da parte dell'autorità giurisdizionale delle relative funzioni (es. in sede d'indagine la raccolta di materiale scientifico probatorio o nelle ipotesi di arresto e di fermo l'eventuale redazione dei documenti correlati).

Un'ipotesi particolare potrebbe essere quella dell'utilizzo dei dati biometrici per verificare l'accesso dei dipendenti, ad aree sensibili o per l'utilizzo di apparati e macchinari pericolosi, da parte del datore di lavoro. In questa ipotesi, nel rispetto dell'art. 4 della legge del 1970 n. 300 (" Statuto dei lavoratori"), è necessario informare i dipendenti sull'utilizzo di questo tipo di dati per le finalità previste da parte della legge.

2.4.7. Dati indicativi della vita o dell'orientamento sessuale

In ultima analisi, bisogna prendere in considerazione i dati che permettono, al titolare o al Responsabile del trattamento, di acquisire conoscenza sulla vita e l'orientamento sessuale dell'interessato. Una delle ipotesi che possiamo prendere in considerazione riguarda l'utilizzo, anche attraverso piattaforme digitali, di agenzie matrimoniali all'interno delle quali dopo aver redatto uno specifico profilo utente (nel quale, solitamente, uno dei dati richiesti riguarda proprio l'orientamento sessuale in ragione delle finalità di ricerca dell'eventuale partner), è possibile autorizzare l'utilizzo di queste informazioni per individuare potenziali partner. È evidente che, in questo caso, la legittimità può essere rinvenuta nel solo consenso esplicito dell'interessato, il quale però dovrà essere adeguatamente informato sul trattamento dei dati stessi e sul loro utilizzo.

2.5. L'informativa all'interessato

L'informativa, ai sensi degli articoli 13 e 14 del GDPR, deve essere fornita all'interessato prima della raccolta dei dati personali, se questi sono stati raccolti presso l'interessato. Se, invece, i dati personali non sono raccolti presso l'interessato, l'informativa deve indicare le categorie di dati personali che saranno oggetto di trattamento e fornire detta informativa entro un termine ragionevole dall'ottenimento dei dati personali e comunque entro un mese.

L'informativa deve contenere almeno le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del DPO;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- le categorie di dati personali in questione (solo nel caso in cui i dati non siano raccolti presso l'interessato);
- i legittimi interessi perseguiti dal titolare del trattamento o da terzi se questi costituiscono la base giuridica del trattamento;
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- l'eventuale trasferimento dei dati in un territorio al di fuori dell'Unione Europea, e, se e quali misure sono state o saranno attuate al fine di garantire un trattamento lecito e sicuro dei dati in conformità di quanto stabilito dal GDPR;
- il periodo di conservazione dei dati o i criteri utilizzati per determinarlo;
- 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 o di opporsi al trattamento, oltre al diritto alla portabilità dei dati;
- nel caso in cui il trattamento si basi sul consenso dell'interessato, l'esistenza del diritto di revocare il consenso in qualsiasi momento;
- il diritto di proporre reclamo a un'autorità di controllo;

- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione del contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze prevista di tale trattamento per l'interessato.

L'Informativa deve essere concisa, trasparente, intelligibile e facilmente accessibile. L'Informativa deve essere resa con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, elettronici. Le informazioni possono essere fornite anche oralmente.

Il GDPR consente di informare gli interessati anche mediante icone standardizzate in combinazione con un'informativa estesa. Le icone standardizzate dovranno essere uguali in tutta l'Unione Europea e saranno definite dalla Commissione Europea. Il titolare è esonerato nel fornire l'Informativa in talune circostanze ed in particolare:

- qualora e nella misura in cui l'interessato disponga già delle informazioni;
- qualora la comunicazione di tali informazioni risulterebbe impossibile o implicherebbe uno sforzo sproporzionato o rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento dovrà adottare le misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
- quando l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare e prevede misure appropriate per tutelare gli interessi legittimi dell'interessato;
- 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.

2.6. Diritti degli interessati

Oltre al diritto all'informativa, come visto al paragrafo precedente, gli articoli dal 12 al 22 del GDPR prevedono specifici diritti per gli interessati, come di seguito elencati:

- diritto di accesso;
- diritto di rettifica;
- diritto di cancellazione (c.d. diritto all'oblio);
- diritto di limitazione di trattamento;
- diritto di portabilità dei dati;
- diritto di opposizione;
- diritto di non essere sottoposto a processi decisionali automatizzati.

2.6.1. Diritto di accesso

Ciascun interessato ha diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardando e, se è in corso tale trattamento, l'acceso ai dati e alle seguenti informazioni:

- finalità del trattamento;
- le categorie di dati personali in questione;
- 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;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;
- 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;
- il diritto di proporre reclamo ad un'autorità di controllo;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica

utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2.6.2. Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano nonché di ottenere l'integrazione dei dati personali incompleti.

2.6.3. Diritto di cancellazione (c.d. diritto all'oblio)

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano nel caso in cui ricorra uno dei seguenti motivi:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento, se non esiste alcun altro motivo legittimo per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun ulteriore motivo legittimo per proseguire il trattamento;
- i dati personali sono stati trattati illecitamente;
- 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;
- i dati personali sono stati raccolti relativamente all'offerta diretta di servizi della società dell'informazione prestati in favore di minori.

Il titolare del trattamento dovrà cancellare senza ingiustificato ritardo i dati personali dell'interessato, astenendosi da ogni ulteriore trattamento e, qualora i dati siano stati resi pubblici dal titolare medesimo, adottare misure ragionevoli (anche tecniche) volte ad informare ogni altro titolare che sta trattando i medesimi dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Il titolare non deve dare seguito alla richiesta di cancellazione nella misura in cui il trattamento venga effettuato:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'UE 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;
- per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all' articolo 89 (1) GDPR, nella misura in cui l'esercizio del diritto alla cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2.6.4. Diritto di limitazione al trattamento

L'interessato ha diritto ad ottenere dal titolare del trattamento la limitazione - ossia la sospensione temporanea che può anche diventare permanente - del trattamento dei propri dati personali, qualora ricorra una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare per verificare l'esattezza di tali dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché il titolare 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;
- l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, (ossia al trattamento necessario per l'esecuzione di un compito di interesse pubblico o basato sul legittimo interesse del titolare, compresa la profilazione), in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare rispetto a quelli dell'interessato.

Al fine di operare concretamente la limitazione al trattamento il titolare può, ad esempio:

- trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento;
- rendere i dati personali selezionati inaccessibili agli utenti;
- rimuovere temporaneamente i dati pubblicati da un sito web.

Nel caso in cui i dati personali oggetto di limitazione siano stati trasmessi ad altri soggetti, è onere del titolare darne comunicazione a ciascuno dei destinatari, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

2.6.5. Diritto di portabilità dei dati

L'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad 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.

Il titolare del trattamento non è responsabile della liceità del trattamento effettuato dal titolare ricevente, non è tenuto a verificare la qualità dei dati prima della relativa trasmissione e non è obbligato a conservare i dati personali per un periodo eccedente i limiti temporali di conservazione al fine di poter dar seguito a potenziali future richieste di portabilità.

Il titolare deve invece implementare procedure specifiche volte a consentire agli interessati di esercitare il diritto alla portabilità.

2.6.6. Diritto di opposizione

L'interessato può in qualsiasi momento opporsi, per motivi connessi alla sua situazione particolare, al trattamento dei propri dati personali che lo riguardano quando il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o quando il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi. Il titolare può continuare il trattamento se dimostra 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 di giudiziaria.

Qualora i dati personali sono trattati per finalità di marketing diretto, l'interessato ha diritto di opporsi al trattamento dei dati personali senza l'obbligo di addurre alcuna motivazione.

Il diritto di opposizione è diverso dal diritto di cancellazione in quanto l'interessato, opponendosi, inibisce al titolare unicamente un determinato utilizzo dei propri dati (quale, ad esempio, l'uso per finalità di marketing), mentre la rimozione assoluta del dato potrebbe provocare conseguenze negative all'interessato, impedendo, ad esempio, al titolare del trattamento di adempiere a eventuali obblighi contrattuali.

Il GDPR prevede espressamente che, nel contesto dei servizi della società dell'informazione, deve essere concessa la possibilità all'interessato di esercitare il diritto di opposizione con mezzi automatizzati.

2.6.7. Diritto di non essere sottoposto a processi decisionali automatizzati

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.

Il diritto non è applicabile nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- 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;
- si basi sul consenso esplicito dell'interessato.

2.7. Approccio basato sul rischio e accountability

Il principio di accountability rappresenta una delle principali novità introdotte dal GDPR, in quanto comporta, ai fini dell'esimente di responsabilità in capo ai titolari del trattamento, la capacità di essere in grado di dimostrare l'adozione delle regole e delle misure previste dal GDPR. Non sarà quindi più sufficiente implementare le regole previste, ma bisognerà documentare i processi, i comportamenti specifici e le azioni concrete finalizzate ad assicurare l'applicazione del GDPR.

Tra le attività da porre in essere si registrano:

- l'adozione di un approccio basato sul rischio con la necessità, attraverso un apposito processo di valutazione, di analizzare i rischi inerenti il trattamento dei dati e l'identificazione di misure tecniche e organizzative di sicurezza adeguate per mitigare i rischi riscontrati;
- l'effettuazione di una valutazione dell'impatto sulla protezione dei dati personali (DPIA) nei casi previsti dal GDPR;
- nella progettazione dei trattamenti occorrerà tenere presente, e garantire, la protezione dei dati personali sin dal nascere del progetto (privacy by design) impostando il trattamento in modo tale da garantire a priori la protezione del dato personale e i diritti degli interessati, ad esempio evitando la raccolta di dati non necessari mediante il tracciamento costante della localizzazione dell'utente di un'app, o il vincolo al rilascio di consensi per finalità marketing in caso di richiesta di un preventivo (privacy by default);
- valutare l'adozione e la tenuta di un registro dei trattamenti eventualmente anche quando questo non risultasse obbligatorio;
- valutare la necessità di nominare un responsabile per la protezione dei dati (DPO) eventualmente anche quando questo non risultasse obbligatorio;
- la creazione di una procedura per la gestione delle violazioni dei dati personali (data breach);
- l'adesione a un codice di condotta o a un meccanismo di certificazione;
- la stesura di un organigramma GDPR che identifichi i ruoli del la protezione dei dati all'interno della struttura e impartisca i relativi compiti;
- il mantenimento di programmi di formazione specifici in materia di protezione dei dati personali per il personale autorizzato al trattamento dei dati;
- la programmazione di audit interni per monitorare il rispetto del sistema di regole che il titolare del trattamento si è posto.

Le suddette misure non rappresentano, evidentemente, un elenco esaustivo e ogni titolare del trattamento e ogni responsabile del trattamento dovranno adottare tutte le azioni necessarie ad assicurare il rispetto del GDPR all'interno della propria struttura.

2.8. Trasferimento dei dati verso Paesi terzi e organismi internazionali

L' art. 44 del GDPR come principio generale sancisce che qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui capo V del Regolamento.

Tutte le disposizioni sono applicate al fine di assicurare che il livello di tutela delle persone fisiche garantito dal Regolamento non sia pregiudicato.

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso, innanzitutto, se la Commissione ha deciso che il paese terzo, o un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

In mancanza di una valutazione di adeguatezza il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha offerto garanzie adeguate e a condizione che siano disponibili diritti azionabili degli interessati e mezzi di ricorso effettivi per gli interessati.

Il trasferimento dei dati verso paesi terzi può anche avvenire quando vi siano norme vincolanti d'impresa che però devono essere approvate dall'Autorità di controllo purché:

a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo di imprese o gruppi di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;
b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali;
c) soddisfino tutta una serie di requisiti fra i quali l'indicazione della struttura e delle coordinate di contatto del gruppo d'imprese in questione e di ciascuno dei suoi membri; l'indicazione dei trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali,

il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione; l'applicazione dei principi generali di protezione dei dati; l'indicazione dei diritti dell'interessato in relazione al trattamento dei suoi dati personali e i mezzi per esercitarli ed ancora altri specificati dall' art. 47 del GDPR.

In assenza di queste condizioni, il trasferimento verso un Paese terzo o un organismo internazionale è ammesso solo se:

- l'interessato abbia esplicitamente acconsentito;
- il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico;
- il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trasferimento sia necessario per tutelare interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trasferimento sia effettuato a partire da un registro che, a norme del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

2.9. Sanzioni

Il GDPR ridisegna l'impianto sanzionatorio in tema di privacy nel quale un elemento centrale del nuovo assetto è rappresentato dalle sanzioni amministrative pecuniarie.

Una volta accertata la violazione di alcune norme del GDPR, l'Autorità di controllo competente può individuare delle misure correttive per affrontare la situazione che si è così venuta a creare. Dette misure sono individuate dall'art. 58, paragrafo 2, del GDPR nelle seguenti azioni:

- rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del GDPR;
- rivolgere ammonimenti al titolare del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR;
- ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal GDPR;
- ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del GDPR, se del caso, in una determinata maniera ed entro un determinato termine;
- ingiungere il titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento incluso il divieto di trattamento;
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli artt. 16, 17 e 18 del GDPR e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;
- revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli artt. 42 e 43 del GDPR, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.
- In aggiunta o in luogo di tali misure, l'Autorità di controllo competente può erogare sanzioni amministrative
- L'ammontare della sanzione viene determinato dall'Autorità sulla base dei seguenti elementi:
- la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative

da essi messe in atto ai sensi degli articoli 25 e 32 del GDPR;

- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- le categorie di dati personali interessate dalla violazione;
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, del GDPR nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;
- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Il GDPR fissa poi esclusivamente dei massimali di sanzione, a seconda della violazione perpetuata. Nello specifico:

- una sanzione fino a 10 milioni di Euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei casi di violazione relativi a:
  - gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43 del GDPR;
  - gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43 del GDPR;
  - gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4, del GDPR;
- una sanzione fino a 20 milioni di Euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei casi di violazione relativi a:
  - i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 del GDPR;
  - i diritti degli interessati a norma degli articoli da 12 a 22 del GDPR;
  - i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49 del GDPR;
  - qualsiasi obbligo ai sensi delle legislazioni specifiche adottate dagli Stati membri;
  - l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'Autorità di controllo ai sensi dell'articolo 58, paragrafo 2, del GDPR o il negato accesso in violazione dell'articolo 58, paragrafo 1, del GDPR.

Come già evidenziato, il grado di responsabilità del titolare del trattamento, e quindi l'importo della sanzione amministrativa, dipenderanno anche da alcuni aspetti che attengono ad attività preventive poste in essere dal titolare e, nello specifico:

- se sono state attuate misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione (c.d. privacy by design) o per impostazione predefinita (c.d. privacy by default);
- se sono state adottate misure organizzative che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita a tutti i livelli dell'organizzazione;
- se è stato messo in atto un livello di sicurezza adeguato;
- se le prassi/politiche/procedure pertinenti in materia di protezione dei dati sono conosciute e applicate al livello adeguato di gestione dell'organizzazione.

È quindi evidente che un'adeguata documentazione dei suddetti aspetti può consentire al titolare del trattamento di attenuare o addirittura di evitare la sanzione amministrativa.

3. ORGANIGRAMMA GDPR

3.1. Figure organizzative relative alla protezione dei dati personali - Organigramma GDPR

3.1.1. Titolare del trattamento

Il titolare del trattamento è colui che ha il potere di determinare le finalità ed i metodi di trattamento dei dati personali ed è, quindi, giuridicamente responsabile del rispetto degli obblighi previsti dal GDPR. Il titolare è altresì il soggetto cui vanno indirizzate le richieste di tutela degli interessati al trattamento, in caso di violazione dei diritti.

I principali obblighi del titolare riguardano:

- l'accountability, cioè l'obbligo di assicurare il rispetto degli obblighi del GDPR e di poter comprovare il rispetto degli stessi;
- la nomina del DPO, sia nei casi di obbligo che nei casi in cui lo stesso è facoltativo;
- il rispetto della privacy by design e la privacy by default;
- la tenuta del registro delle attività di trattamento, quando obbligatoria;
- la valutazione di impatto sulla protezione dei dati (DPIA) quando il trattamento può presentare un rischio elevato per i diritti delle persone e, in particolare, nel caso si utilizzino nuove tecnologie;
- la segnalazione delle perdite di dati (data breach);
- il riscontro alle richieste degli interessati.

Nel settore privato il titolare del trattamento può essere una persona fisica oppure una persona giuridica mentre nel settore pubblico il titolare del trattamento è in genere la stessa autorità.

Quanto alle persone giuridiche, il titolare del trattamento è l'ente stesso, a prescindere dall'organo o dalle persone fisiche che ne esprimano la volontà[1].

Nel caso di cui al presente modello, Titolare del trattamento è **SISIFO Consorzio di Cooperative Sociali a r.l.** la quale ha delegato il proprio Referente GDPR all'esercizio dei poteri decisionali e di spesa in materia di trattamento di dati personali, con particolare riguardo all'adozione delle misure di sicurezza previste dalla normativa applicabile.

3.1.2. Responsabile del trattamento

Il responsabile del trattamento è definito dal GDPR come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento. Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate affinché il trattamento rispetti i requisiti del GDPR.

La figura del responsabile del trattamento acquisisce una condizione di maggior professionalità che deve essere preventivamente valutata dal titolare attraverso, ad esempio, la verifica del possesso di certificazioni o dell'adesione a codici di condotta, o ancora sulla base di autodichiarazioni sulle competenze del responsabile in tema di protezione de dati.

I principali obblighi del responsabile riguardano:

- la tenuta dei registri dei trattamenti svolti;
- l'eventuale nomina di un sub-responsabile, previa autorizzazione scritta;
- la nomina del DPR, sia nei casi di obbligo che nei casi in cui lo stesso è facoltativo;
- la comunicazione al titolare del trattamento, qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni nazionali o dell'Unione in

[1] Su questo punto si è espresso il Garante fin dal 1997 con la Circolare n. 291/5 del 13 novembre doc. n. 39785, con la quale si è chiarito che "qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il "titolare" è l'entità nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.), anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.)". Questa posizione del Garante è stata poi cristallizzata nel 2003, con l'emanazione del Codice della Privacy che, all' art. 28, specifica, con parole pressoché identiche a quelle della Circolare del 1997, che "quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza".

tema di protezione dati;

- il rispetto della privacy by design e la privacy by default;
- la segnalazione al titolare delle perdite di dati (data breach);
- l'assistenza al titolare del trattamento nel riscontro alle richieste degli interessati.

I responsabili del trattamento possono essere interni, se inseriti nell'organizzazione aziendale, o esterni, se non inseriti nell'organizzazione.

SISIFO Consorzio di Cooperative Sociali a r.l. ha predisposto la nomina dei responsabili del trattamento, indicando in particolare i seguenti elementi previsti dall'art. 28 del GDPR:

- la materia disciplinata;
- la durata, natura e finalità del trattamento;
- il tipo di dati trattati e la categoria degli interessati;
- l'obbligo del trattamento dei dati solo previa istruzione documentata da parte del titolare del trattamento (salvo che lo richieda il diritto dell'Unione o nazionale cui è sottoposto il trattamento);
- la garanzia che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- l'obbligo che siano adottate tutte le misure richieste per la sicurezza del trattamento, ai sensi dell'art. 32 del GDPR;
- l'obbligo che siano rispettate le condizioni, previste dai paragrafi 2 e 4 dell'art. 28 del GDPR, nell'ambito della nomina di un altro responsabile del trattamento, in particolar modo con la richiesta di un'autorizzazione scritta del titolare in caso di nomina di un sub-responsabile;
- in base alla natura del trattamento, l'obbligo di assistenza al titolare con misure tecniche e organizzative al fine di soddisfare l'obbligo di quest'ultimo di soddisfare le richieste dell'interessato;
- l'obbligo di fornire assistenza al titolare del trattamento nell'ambito degli obblighi che fanno capo al titolare, attinenti alla sicurezza del trattamento ed alla consultazione preventiva;
- l'obbligo, su richiesta del titolare del trattamento, della cancellazione o restituzione di tutti i dati personali al termine della prestazione dei servizi relativi al trattamento, salvo che il diritto dell'Unione o degli Stati membri non preveda la conservazione dei dati;
- l'obbligo di mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal titolare del trattamento o da un soggetto da questi incaricato.

Il Titolare del trattamento, in sede di prima applicazione, ha individuato i seguenti Responsabili del trattamento:

ELENCO RESPONSABILI DEL TRATTAMENTO	
DENOMINAZIONE / RAGIONE SOCIALE	ATTIVITÀ ESTERNALIZZATA
TRAPANI SALVATORE	Consulente del lavoro
BRISCHETTO GIUSEPPE	Consulente fiscale
SCM DATI S.R.L.	Consulente fiscale
4D SOFT S.R.L.	Consulente hardware
SCIACCHITANO CARLO	Medico Competente D. Lgs.vo n. 81/2008
CATALANO ALFIO	Consulente D. Lgs. 81/2008 - RSPP
ICC DIGITAL MEDIA	Consulente Hardware/software (Sito Web)
MERLO ARTURO	Consulente legale
MACRI' ENRICO	Consulente legale
PULIATTI ANTONIO	Consulente legale
GAMBUZZO ALESSIA	ODV
STRAZZERI ALESSIO CIRO	Consulente D. Lgs. 231/2001 - ODV
CAPORLINGUA CARMELO	Consulente Progettazione - Consulente ISO 9001
CHRIELEISON ROSALBA	Consulente Progettazione
GIUFFRIDA MASSIMILIANO	Consulente Progettazione

In ogni caso, la designazione di ulteriori Responsabili del trattamento potrà avvenire utilizzando il modello "Atto di designazione Responsabile del Trattamento dei dati personali" **[MODP.DES02]**.

3.1.3. Autorizzato al trattamento

Il GDPR non prevede espressamente la figura dell'incaricato al trattamento, ma non ne esclude la presenza quando, all'art. 4, n. 10, fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Quindi anche se il GDPR non prevede detta figura autonoma, ciò non impedisce al titolare e al responsabile del trattamento, oltre a fare tutto ciò che il regolamento espressamente prevede per dette persone, di attuare su base volontaria una procedura di ulteriore responsabilizzazione delle stesse attraverso una specifica lettera di attribuzione di incarico identificando dette persone quali incaricati.

Il Titolare del trattamento ha individuato tutti i soggetti che, all'interno all'Organizzazione, trattano dati personali, designandoli Autorizzati al trattamento tramite l'utilizzo di apposito modello [MODP.DES04].

L'elenco del personale dipendente è presente presso l'apposito ufficio della sede amministrativa di Catania. Per ulteriori designazioni si procederà in egual modo.

3.1.4. Responsabile della protezione dei dati (DPO)

Il responsabile della protezione dei dati (DPO) è la figura di riferimento per tutto ciò che attiene al trattamento dei dati personali, sia all'interno dell'azienda od organizzazione, sia nei rapporti esterni della stessa con l'Autorità di controllo e con gli interessati.

La nomina del DPO è obbligatoria:

- per tutti i soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.);
- per i soggetti privati quando la loro attività principale consiste nel monitoraggio regolare e sistematico degli interessati su larga scala oppure nel trattamento su larga scala di categorie particolari di dati personali (quelli sensibili) o relativi a condanne penali e reati.

La nomina del DPO può comunque avvenire anche in via facoltativa.

I compiti del DPO possono essere così sintetizzati:

- consultivo: tra i compiti vi è quello di informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- formativo: spetta al DPO informare, sensibilizzare e formare il personale che partecipa ai trattamenti in merito alla normativa sulla protezione dei dati;
- garanzia: il DPO sorveglia l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali;
- punto di contatto: il DPO funge da interfaccia tra tutti i soggetti coinvolti nella protezione dei dati (Autorità di controllo, interessati, azienda).

Il DPO deve agire in modo autonomo, senza ricevere alcuna istruzione per quanto riguarda lo svolgimento dei propri compiti, e la sua posizione deve essere indipendente rispetto alle altre funzioni dell'organizzazione, e quindi detto ruolo non potrà essere ricoperto da chi all'interno svolge una funzione a livello esecutivo, per evitare che vi siano conflitti di interessi[2].

Il DPO deve altresì possedere adeguate qualità professionali, in particolar modo un adeguato livello di conoscenza specialistica della normativa e della prassi in materia di protezione dei dati. Fra le competenze e conoscenze specialistiche pertinenti rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del GDPR;

[2] Al riguardo il Gruppo Art. 29 precisa che non potranno ricoprire il ruolo di DPO i responsabili della funzione risorse umane, del marketing o dei sistemi informativi.

- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare e/o del responsabile;
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare e/o del responsabile.

SISIFO Consorzio di Cooperative Sociali a r.l. valutato di avere l'obbligo di nomina del DPO in quanto la propria attività consiste nel trattamento su larga scala di categorie particolari di dati personali ha designato, quale Responsabile della Protezione dei Dati Personali (DPO) **SIAPA s.r.l.** nella persona del Sig. **SIRNA GRILLERI Antonino.**

3.1.5. Referente GDPR

Da un'analisi della struttura organizzativa di **SISIFO Consorzio di Cooperative Sociali a r.l.** e della complessità delle problematiche organizzative e tecniche ad essa connesse, si è ritenuto opportuno procedere, anche, alla nomina di un Referente GDPR, che affianchi il DPO e rappresenti per egli un punto di riferimento (c.d. punto di contatto) sia ai fini di eventuali verifiche e controlli sia al fine di consentire un migliore e agevole esercizio dei diritti degli interessati.

Il Referente GDPR collabora, altresì, per le attività formative, informative e di monitoraggio, e rappresenta il principale punto di riferimento tra il DPO ed il Titolare del trattamento nella gestione del trattamento dei dati personali interno alla struttura.

SISIFO Consorzio di Cooperative Sociali a r.l. ha nominato, quale Referente GDPR:

- **SEDE DI MESSINA (A.D.I.P.)**
- ✓ *per l'ambito Sanitario:* ***MAZZEI Micol***
- ✓ *per l'ambito Amministrativo:* ***GERMANÀ Antonio***
- **SEDE DI CATANIA (AMMINISTRAZIONE)**
- ✓ *per l'ambito Sanitario:* ***TESTAÌ Caterina***
- ✓ *per l'ambito Amministrativo:* ***GOTTARDI Bruna***
- **SEDE DI CALTANISSETTA (A.D.I.P.)**
- ✓ *per l'ambito Sanitario e Amministrativo:* ***BARONE Lorenzo***
- **SEDE DI AGRIGENTO (A.D.I.P.)**
- ✓ *per l'ambito Sanitario e Amministrativo:* ***BOE Laura***
- **SEDE DI AGRIGENTO (A.D.I.)**
- ✓ *per l'ambito Sanitario:* ***MARCIANTE Irene***
- ✓ *per l'ambito Amministrativo:* ***BAIO Salvatore***

3.1.6. Amministratore di Sistema

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del trattamento dei dati personali, anche in forza del provvedimento del garante del 27 novembre 2008, vengono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.
La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una

circostanza aggravante. Ci si riferisce, in particolare, all'abuso della qualità di operatore di sistema prevista dal codice penale per le fattispecie di accesso abusivo a sistema informatico o telematico (art. 615 ter) e di frode informatica (art. 640 ter), nonché per le fattispecie di danneggiamento di informazioni, dati e programmi informatici (artt. 635 bis e ter) e di danneggiamento di sistemi informatici e telematici (artt. 635 quater e quinques) di recente modifica.

La disciplina di protezione dei dati previgente al Codice del 2003 definiva l'amministratore di sistema, individuandolo quale "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Il Codice non ha invece incluso questa figura tra le proprie definizioni normative. Tuttavia le funzioni tipiche dell'amministrazione di un sistema sono richiamate nel menzionato Allegato B, nella parte in cui prevede l'obbligo per i titolari di assicurare la custodia delle componenti riservate delle credenziali di autenticazione. Gran parte dei compiti previsti nel medesimo Allegato B spettano tipicamente all'amministratore di sistema: dalla realizzazione di copie di sicurezza (operazioni di backup e recovery dei dati) alla custodia delle credenziali alla gestione dei sistemi di autenticazione e di autorizzazione.

Nel loro complesso, le norme predette mettono in rilievo la particolare capacità di azione propria degli amministratori di sistema e la natura fiduciaria delle relative mansioni, analoga a quella che, in un contesto del tutto differente, caratterizza determinati incarichi di custodia e altre attività per il cui svolgimento è previsto il possesso di particolari requisiti tecnico-organizzativi, di onorabilità, professionali, morali o di condotta, a oggi non contemplati per lo svolgimento di uno dei ruoli più delicati della "Società dell'informazione".

Nel corso delle attività ispettive disposte negli ultimi anni dal Garante è stato possibile rilevare quale importanza annettano ai ruoli di system administrator (e di network administrator o database administrator) la gran parte di aziende e di grandi organizzazioni pubbliche e private, al di là delle definizioni giuridiche, individuando tali figure nell'ambito di piani di sicurezza o di documenti programmatici e designandoli a volte quali responsabili.

In altri casi, non soltanto in organizzazioni di piccole dimensioni, si è invece riscontrata, anche a elevati livelli di responsabilità, una carente consapevolezza delle criticità insite nello svolgimento delle predette mansioni, con preoccupante sottovalutazione dei rischi derivanti dall'azione incontrollata di chi dovrebbe essere preposto anche a compiti di vigilanza e controllo del corretto utilizzo di un sistema informatico.

Con il presente provvedimento il Garante intende pertanto richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema.

L'Autorità ravvisa inoltre l'esigenza di individuare in questa sede alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito di organizzazioni ed enti pubblici e privati, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

SISIFO Consorzio di Cooperative Sociali a r.l. ha nominato, quale amministratore di sistema, **per tutte le sedi, il Dott. RUSSO ANTONIO.**

3.1.7. Organigramma GDPR

Sulla base delle figure indicate nei paragrafi, si è quindi sviluppato quindi l'organigramma GDPR, dettagliato nel documento "Organigramma GDPR" **[MODP.ODP]** allegato al presente modello.

4. IL MODELLO ORGANIZZATIVO DATA PROTECTION DI SISIFO CONSORZIO DI COOPERATIVE SOCIALI A R.L.

4.1. Premessa

L'adozione di un Modello Organizzativo Data Protection, che sia adeguato a quanto prescritto dal GDPR, rappresenta uno dei modi attraverso il quale l'Associazione può dimostrare il rispetto del principio di responsabilizzazione (accountability), ed evitare quindi le pesanti sanzioni previste dal Regolamento.

SISIFO Consorzio di Cooperative Sociali a r.l. ha, quindi, inteso avviare una serie di attività finalizzate ad una adozione di un proprio Modello e volte a rendere e mantenere lo stesso quanto più possibile allineato ai requisiti previsti dal GDPR e coerente con i principi già radicati nella propria cultura di governo dall'Organizzazione.

Tale processo di adozione ha comportato un'articolata analisi dell'operatività di **SISIFO Consorzio di Cooperative Sociali a r.l.**, anche mediante un'attività di risk assessment focalizzata sulla verifica dei rischi inerenti al trattamento dei dati personali, ispirandosi all'approccio metodologico schematicamente descritto nei paragrafi che seguono.

Le risultanze di tale processo di analisi hanno prodotto il presente Modello Organizzativo Data Protection e i documenti ad esso allegati.

4.2. L'approccio metodologico per la definizione del Modello Organizzativo Data Protection

La metodologia scelta per l'adozione del Modello, in termini di organizzazione, definizione delle modalità operative, strutturazione in fasi ed assegnazione delle responsabilità tra le varie funzioni aziendali, è definita da **SISIFO Consorzio di Cooperative Sociali a r.l.** al fine di garantire la qualità e l'autorevolezza dei risultati.

L'attività si sviluppa nelle seguenti fasi metodologiche sinteticamente riassunte nella tabella che segue:

FASI	ATTIVITÀ
Fase 1	**Inventario dei dati (Data inventory)** La prima fase di costruzione di un modello organizzativo volto alla protezione dei dati personali passa necessariamente dalla verifica di quali sono i dati trattati e i trattamenti in atto all'interno dell'Organizzazione.
Fase 2	**Valutazione d'impatto sulla protezione dei dati** Posto che **SISIFO Consorzio di Cooperative Sociali a r.l.** ha valutato che la natura, l'oggetto, il contesto e le finalità del trattamento possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche, viene redatta una valutazione d'impatto al fine di valutare gli effetti del trattamento sulla protezione dei dati personali.
Fase 3	**Analisi dei rischi (Risk assessment)** Una volta individuati i dati e i relativi trattamenti, è necessario analizzare i rischi relativi a detti dati, costruendo una matrice dei rischi che consenta di associare ad ogni rischio una probabilità del verificarsi dell'evento e un danno potenziale ad esso associato.
Fase 4	**Piano di azione (Action Plan)** Una volta individuati i rischi, viene redatto un piano di azione che identifichi le misure organizzative e tecniche necessarie alla riduzione dei rischi identificati nella precedente analisi. Il piano di azione terrà conto sia dell'urgenza dell'intervento che della sua sostenibilità.
Fase 5	**Implementazione delle misure organizzative** L'implementazione delle misure organizzative riguarderà, ad esempio, la definizione dell'organigramma privacy, l'attuazione di politiche, procedure e linee guida, la redazione di un codice etico, l'adeguamento di contratti e informative, l'attivazione di procedure specifiche per la gestione dei rapporti con gli interessati e con le terze parti e l'attivazione di procedure per il data breach management.

Fase 6	**Implementazione delle misure tecniche** In aggiunta alle misure organizzative, e per completare e implementare le stesse, andranno adottate anche adeguate misure tecniche che consentano di raggiungere gli obiettivi del GDPR e ridurre i rischi identificati. Si segnalano, ad esempio, le politiche di backup, l'adeguamento tecnologico di hardware e software, l'intervento sui siti internet e i profili social e le attività di pseudonimizzazione.
Fase 7	**Formazione e informazione** L'adeguamento ai principi e ai contenuti del GDPR passa anche attraverso la piena consapevolezza dell'intera struttura in merito alle problematiche connesse con il Regolamento e al contenuto del Modello Organizzativo Data Protection adottato dall'Organizzazione. Questa consapevolezza viene raggiunta attraverso idonee attività formative verso tutti i soggetti facenti parte dell'Organizzazione.
Fase 8	**Monitoraggio** Il Modello Organizzativo Data Protection e la sua implementazione vanno costantemente verificati al fine di accertare che vengano mantenuti i requisiti di compliance rispetto al GDPR.

4.2.1. Inventario dei dati - Data inventory (Fase 1)

La fase di inventario dei dati si sviluppa attraverso una valutazione della situazione generale dell'Ente in termini di rispetto della privacy cui segue, previo accesso presso la struttura, attraverso la compilazione di una serie di check-list, l'inventario dei trattamenti in essere e i dati personali trattati, individuando i seguenti dati minimi:

- la finalità del trattamento
- le categorie di interessati (indicando se trattasi di soggetti minori)
- le categorie di dati personali (indicando la tipologia, la fonte e la base giuridica)
- i destinatari cui i dati sono o saranno comunicati (indicando se trattasi di destinatari situati in paesi terzi o organizzazioni internazionali)
- la modalità di raccolta del consenso
- i soggetti coinvolti nel trattamento
- i termini ultimi previsti per la cancellazione delle singole categorie di dati
- il luogo in cui i dati vengono conservati
- le misure tecniche e organizzative adottate (ad es. policies, istruzioni, procedure ecc.).

I suddetti dati sono stati trasfusi in un documento riepilogativo, denominato "Identificazione delle Risorse da Proteggere e Misure di Sicurezza" **[MODP.IRP]**.

Parallelamente, al fine di poter predisporre una corretta analisi dei rischi e un adeguamento idoneo ai principi statuiti al GDPR, viene effettuato anche un inventario degli asset tecnologici e del sistema informativo aziendale (ad es. elenco degli applicativi, dei database, dell'hardware utilizzato ecc.), in quanto necessario al fine di individuare le misure tecniche e organizzative idonee al rispetto del Regolamento.

Si è quindi operata una raccolta ed esame dei dati e delle informazioni disponibili allo scopo di identificare i meccanismi operativi dei processi a potenziale rischio privacy nonché di predisporre un modello che fosse il più possibile cucito sulla realtà della struttura.

Si è, altresì, proceduto a istituire il "Registro delle attività di trattamento" effettuato dal Titolare **[MODP.RAT]** ai sensi dell'art. 30 comma 1 del GDPR, nel quale sono indicati:

REGISTRO	Titolare del trattamento
Contatti	Nome e dati di contatto del Titolare del trattamento
Denominazione del trattamento	Per ogni tipologia di trattamento, le attività di trattamento svolte sotto la propria responsabilità
Ufficio / Funzione / Unità Organizzativa	Per ogni tipologia di trattamento, l'ufficio, funzione e/o unità organizzativa incaricata di gestire i dati personali relativi allo specifico trattamento
Finalità del trattamento	Per ogni tipologia di trattamento, l'indicazione delle finalità del trattamento
Categorie di dati personali	Per ogni tipologia di trattamento, una descrizione delle categorie di dati personali

Categorie particolari di dati personali	Se per quella specifica attività di trattamento vengono trattati dai particolari, l'elencazione dei suddetti dati divisi per categorie
Categorie degli interessati	Per ogni tipologia di trattamento, l'elenco delle categorie di interessati in relazione alla specifica attività di trattamento
Destinatari delle comunicazioni dei 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. In quest'ultimo caso è stato indicato il paese terzo o l'organizzazione internazionale destinataria e le garanzie adottate a tutela degli interessati per il suddetto trasferimento
Base giuridica	Per ogni attività di trattamento viene indicata la base giuridica o le basi giuridiche che, ai sensi del GDPR, rendono lecito il trattamento dei dati
Termini di cancellazione	I limiti di conservazione e di successiva cancellazione delle diverse categorie di dati
Modalità di raccolta dei dati personali	Viene indicata la modalità attraverso i dati personali per quella specifica attività di trattamento sono stati raccolti (es. presso gli interessati, presso terzi, ecc.)
Modalità di raccolta del consenso degli interessati	Nel caso in cui la base giuridica sia anche il consenso dell'interessato, per alcune specifiche attività di trattamento, viene indicata la modalità di raccolta del consenso (ad es. per iscritto)
Misure di sicurezza	Le misure di sicurezza tecniche e organizzative adottate per garantire un livello di sicurezza adeguato

È stata infine redatta un'apposita procedura di "Predisposizione, composizione e gestione del Registro delle Attività di trattamento" **[MODP.PR001].**

4.2.2. Valutazione d'impatto sulla protezione dei dati (Fase 2)

Così come previsto dall'art. 35 del GDPR, il Titolare del trattamento, considerata la natura, l'oggetto, il contesto e le finalità del trattamento, ha ritenuto necessario, prima di procedere al trattamento, operare una valutazione d'impatto sulla protezione dei dati al fine di verificare l'eventuale esistenza di un rischio elevato per i diritti e le libertà delle persone fisiche.

In particolar modo si è ritenuto che, ai sensi dell'art. 35, paragrafo 3, si rientrasse nei seguenti casi di obbligo di valutazione di impatto:

- lett. b) – trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- lett. c) – sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione è stata condotta esclusivamente sulle tipologie di trattamento che si è ritenuto potessero presentare rischi elevati per i diritti e le libertà delle persone fisiche ed è avvenuta con la consultazione del responsabile della protezione dei dati.

In funzione di ciò si è costruita una valutazione di impatto, rinvenibile nel documento "Valutazione d'Impatto sulla protezione dei dati (DPIA)" **[MODP.VIA]**, contenente i seguenti elementi:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Nell'esecuzione della valutazione d'impatto, si è tenuto conto delle "Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del regolamento 2016/679" emanate dal gruppo di lavoro WP29, anche attraverso l'utilizzo del software per la valutazione d'impatto messo a disposizione del Garante per la privacy.

All'esito della valutazione d'impatto, si ritiene che le misure tecniche e organizzative adottate o in corso di adozione, anche in seguito all'analisi di cui

al successivo punto 4.2.3., riducano il rischio ad un livello accettabile e non è quindi necessario procedere alla consultazione dell'autorità di controllo ai sensi dell'art. 36.

4.2.3. Analisi dei rischi - Risk assessment (Fase 3)

Così come previsto dall'art. 32 del GDPR, il Titolare del trattamento, 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, deve mettere in atto misure tecniche e organizzative che garantiscano un livello di sicurezza adeguato al rischio, tenuto conto in special modo dei rischi presentati dal trattamento che derivano in particolare da:

- distruzione
- perdita
- modifica
- divulgazione non autorizzata
- accesso accidentale o illegale

4.2.3.1. Metodologia di analisi del rischio

Il rischio può essere considerato, secondo la norma ISO 31000 "Gestione del rischio", come l'effetto dell'incertezza sugli obiettivi, e tale definizione è in linea con il concetto comune che lega il rischio alla probabilità e all'impatto: il rischio è tanto più grande quanto è più probabile che l'evento collegato si verifichi e quanto maggiore è l'effetto del verificarsi dell'evento. Anche il GDPR, all'art. 32, richiama quindi i medesimi concetti quando parla di "rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" e gli stessi vengono ripresi nelle linee guida del Gruppo di lavoro Articolo 29 che definisce il rischio "uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità".

L'analisi dei rischi richiede quindi, per ogni tipologia di rischio, la valutazione della probabilità che lo stesso si verifichi e dell'impatto ad esso collegato. Nello specifico, ai fini del presente documento, si intenderà:

- per probabilità la possibilità che un evento si verifichi
- per impatto la magnitudo degli effetti collegati all'evento

Per ogni rischio/evento dannoso (distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale) andrà quindi verificato:

- il potenziale impatto sui dati del verificarsi dell'evento e la magnitudo del potenziale impatto
- le minacce che possono determinare il verificarsi dell'evento e le fonti di rischio che possono causarle
- la probabilità che l'evento dannoso si verifichi

Preliminarmente è stata quindi costruita una matrice del livello di rischio, come prodotto della probabilità e dell'impatto.

L'impatto è stato graduato secondo la seguente scala:

IMPATTO		
1	Trascurabile	Il verificarsi dell'evento non può provocare alcun danno o solo un danno minimo che può essere facilmente riparato (es. perdite di tempo per il reinserimento dei dati, irritazione, ecc.)
2	Limitato	Il verificarsi dell'evento può provocare un danno che può essere riparato con uno sforzo limitato (es. costi aggiuntivi, interruzione dell'attività, stress, ecc.)
3	Significativo	Il verificarsi dell'evento può provocare un danno che può essere riparato con grave difficoltà (es. appropriazione di fondi, danno alla proprietà, perdita di lavoro, causa civile, ecc.)
4	Massimo	Il verificarsi dell'evento può provocare un danno irreparabile (es. fallimento, cessazione dell'attività, ecc.)

La probabilità è stata graduata secondo la seguente scala:

PROBABILITÀ		
1	Trascurabile	Il verificarsi dell'evento non appare possibile (es. furto di documenti da una stanza il cui accesso è protetto da lettore di badge e codice identificativo)
2	Limitata	Il verificarsi dell'evento appare di difficile (es. furto di documenti da una stanza il cui accesso è protetto da lettore di badge)
3	Significativa	Il verificarsi dell'evento appare possibile (es. furto di documenti da una stanza sita in un locale nel quale si accede previo passaggio dalla reception)
4	Massima	Il verificarsi dell'evento appare probabile (es. furto di documenti da una stanza senza alcuna misura di sicurezza).

La valutazione del rischio è espressa nella seguente formula:

Rischio (R) = Probabilità (P) x Impatto (I)

Al fine di determinare l'esposizione si è utilizzata la seguente matrice:

PROBABILITÀ						
	Massima	4	4	8	12	16
	Significativa	3	3	6	9	12
	Limitata	2	2	4	6	8
	Trascurabile	1	1	2	3	4
			1	2	3	4
			Trascurabile	Limitato	Significativo	Massimo
			IMPATTO			

Infine, si è costruito l'elenco dei rischi, suddividendoli in 3 macro-aree:

- rischi relativi all'ambiente fisico
- rischi relativi al comportamento degli operatori
- rischi relativi agli strumenti utilizzati (hardware e software)

Per ogni rischio è stato indicato il tipo di evento potenzialmente associato (distruzione, perdita, modifica, divulgazione, accesso), il rischio valutato secondo la precedente tabella, le misure di sicurezza in essere, le misure di sicurezza da adottare e il rischio residuo derivante dall'adozione delle suddette misure.

Il risultato dell'analisi è stato trasfuso nel documento "Analisi dei rischi ed Action Plan" **[MODP.ADR]**.

4.2.4. Piano di azione – Action Plan (Fase 4)

Una volta effettuata la mappatura dei dati e l'analisi dei rischi, si è proceduto con la definizione di un piano di azione per la riduzione dei rischi rilevati, catalogando gli interventi in base alla loro urgenza (valutata in base al rischio esistente e al gap tra situazione attuale e situazione ottimale) e alla loro sostenibilità (valutata sulla base dei costi di realizzazione, sia in termini prettamente economici che di impatto sull'organizzazione e sull'impianto tecnologico, e delle difficoltà di implementazione).

É stata quindi redatta una pianificazione di interventi da effettuare, dando maggior priorità a quelli più urgenti e più facilmente realizzabili e poi passando, via via a quelli non urgenti e facilmente realizzabili, a quelli urgenti ma che richiedono un impegno economico/organizzativo più imponente, valutando poi la realizzabilità degli interventi non urgenti e scarsamente sostenibili.

Il risultato di detta analisi, e della relativa pianificazione, viene riassunto nel documento "Analisi dei rischi ed Action Plan" **[MODP.ADR].**

4.2.5. Implementazione delle misure organizzative (Fase 5)

Tra le misure organizzative necessarie ai fini del rispetto del GDPR, individuate nell'ambito del Piano di azione, si possono elencare:

- individuazione delle figure chiave ai fini del trattamento dei dati personali, con contestuale redazione del documento "Organigramma GDPR" **[MODP.ODP]**
- la redazione di una procedura per il "Rilascio e gestione delle designazioni o nomine" **[MODP.PR003]** e la conseguente nomina delle figure chiave ai fini del trattamento dei dati personali quali:
  - responsabile della protezione dei dati personali;
  - responsabili del trattamento;
  - referente GDPR;
  - amministratore di sistema;
  - autorizzati al trattamento;
  - custode dell'archivio ad accesso controllato
  - medico competente per i lavoratori dipendenti sottoposti a sorveglianza sanitaria
- la redazione di una procedura per la "Gestione delle informative e dei consensi al trattamento" **[MODP.PRO.02]** e la conseguente redazione e consegna delle informative a:
  - Informativa Assistiti
  - Informativa Volontari
  - Informativa Fornitori
  - Informativa Personale Dipendente
  - Informativa Tirocinanti
  - Informativa Liberi professionisti
  - Enti Strumentali
  - Cooperative sociali
- l'acquisizione del consenso dell'interessato quando necessario
- l'adozione di un'apposita procedura per la "Gestione delle richieste degli interessati al trattamento" **[MODP.PR004]**
- l'adozione di un'apposita procedura per la "Gestione del data breach" **[MODP.PR007]**

L'elenco delle misure organizzative identificate è comunque inserito nel documento "Analisi dei rischi ed Action Plan" **[MODP.ADR]**.

4.2.6. Implementazione delle misure tecniche (Fase 6)

In uno con le misure organizzative, **SISIFO Consorzio di Cooperative Sociali a r.l.** deve adeguare la propria struttura tecnologica. A tal fine viene programmata un'attività di adeguamento che tenga conto, tra le altre cose:

- della necessità di una gestione unificata dell'identità e dei profili di accesso degli utilizzatori dei dati e del tracciamento delle loro attività (logging);
- della capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di rilevare eventi ed incidenti, riconducibile al tema della gestione dei data breach;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (ad es. adeguate infrastrutture per il backup e il restore);
- la creazione di procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche al fine di garantire la sicurezza del trattamento.

Tra le misure applicative dei suddetti principi, va dedicata una particolare attenzione:

- all'integrazione dei sistemi applicativi con il sistema di gestione delle identità e dei profili di accesso;

- alla pseudonimizzazione;
- alla cifratura dei dati;
- al mantenimento di misure di sicurezza informatica adeguate come, ad esempio:
- firewall;
- instrusion detection system ("IDS");
- intrusion prevention systems (IPS");
- sistemi di monitoraggio degli eventi di sicurezza;
- antivirus
- al mantenimento di misure di sicurezza fisica adeguate come, ad esempio:
- videosorveglianza;
- barriere protettive;
- guardie;
- lucchetti;
- altre misure di protezione degli asset fisici
- la creazione di una procedura di prevenzione della perdita dei dati, integrata con adeguati strumenti di backup e restore.

L'elenco delle misure tecniche identificate è inserito nel documento "Analisi dei rischi ed Action Plan" **[MODP.ADR]**.

4.2.7. Formazione e informazione (Fase 7)

L'attività di formazione e informazione del personale coinvolto nell'attività di trattamento di dati personali dovrà avvenire già sin dal momento dell'assunzione, sia attraverso la fornitura di specifiche istruzioni e di materiale informativo sul GDPR (vedi lo specifico "Opuscolo informativo" **[MODP.OPI]**, sia attraverso degli appositi corsi di formazione, svolti di norma con cadenza annuale, salvo che modifiche normative e/o organizzative non necessitino di corsi specifici da svolgersi con frequenza più ristretta. La formazione dovrà essere preventiva rispetto all'inizio dell'attività di trattamento da parte del singolo dipendente.

L'attività di formazione deve essere affidata a soggetti qualificati, dovrà essere indirizzata a tutto il personale di **SISIFO Consorzio di Cooperative Sociali a r.l.**, e andrà documentata con la compilazione di un apposito "Registro corso di formazione" **[MODP.MOD30]** nel quale andranno registrati i nominativi dei soggetti presenti al corso, con firma di entrata ed uscita, il nominativo dei relatori e l'indicazione degli argomenti trattati. Al termine del corso di formazione dovrà altresì essere somministrato almeno un test finale al fine di valutare la comprensione degli argomenti da parte dei partecipanti.

La formazione dovrà essere finalizzata ad illustrare in particolare i rischi generali e specifici dei trattamenti dei dati, le misure organizzative, tecniche ed informatiche adottate, nonché le responsabilità e le sanzioni.

L'obbligo di effettuare un'adeguata formazione spetta al Titolare del trattamento, il quale lo assolverà di concerto con il Referente GDPR, il quale ha uno specifico obbligo di informazione verso i dipendenti e di controllo sulla formazione effettuata dal Titolare del trattamento.

4.2.8. Monitoraggio (Fase 8)

Un elemento essenziale per garantire l'efficacia nel tempo di un Modello Organizzativo Data Protection è quello del monitoraggio, che consente di verificare che le misure organizzative e tecniche adottate garantiscono un livello di sicurezza adeguato al rischio.

Il Titolare del trattamento, coadiuvato dal Referente GDPR e dalle altre figure interne alla struttura e impegnate nel trattamento e la protezione dei dati, dovrà porre in essere una serie di attività di monitoraggio documentate, al fine di effettuare la superiore verifica.

Dette attività potranno consistere, a titolo esemplificativo:

- nell'esecuzione di audit interni, con cadenza regolare, al fine di verificare se l'organizzazione rispetta le policy interne e le procedure stabilite. Al termine di tale analisi possono essere prese decisioni di creazione o aggiornamento delle policy, di creazione o adattamento delle procedure, di esecuzione di ulteriori attività formative ecc.;
- effettuare controlli a sorpresa al fine di verificare il rispetto delle policy interne;

- simulare una richiesta da parte di un interessato per verificare il corretto funzionamento delle procedure di risposta;
- simulare una perdita di dati per verificare il corretto funzionamento delle procedure di risposta ai data breaches;
- simulare un accesso non autorizzato, anche informatico, ai dati;
- verifica delle clausole contrattuali e dell'esistenza dei consensi per i trattamenti dei dati.