6. ASPETTI OPERATIVI

Il presente vademecum si propone di fornire ai professionisti sanitari una guida pratica per gestire in modo corretto ed efficace l'attività clinico-assistenziale, con particolare attenzione alla tutela dei dati personali e alla qualità della documentazione prodotta, nel rispetto del Regolamento Europeo 2016/679 (GDPR).

Per garantire una pratica professionale conforme agli standard normativi e deontologici, è fortemente consigliato dotarsi dei seguenti strumenti operativi:

- **Documentazione clinico-assistenziale**: strumento imprescindibile per tracciare in modo sistematico e sicuro tutte le attività svolte a favore del paziente. La documentazione deve essere redatta in forma chiara, completa e aggiornata, rispettando i principi di minimizzazione, esattezza e conservazione dei dati previsti dal GDPR.
- **Consenso informato**: sebbene la normativa talvolta consenta di prescindere dalla forma scritta, è consigliabile acquisire il consenso informato del paziente in modalità documentata, per attestare l'avvenuta informazione e la libera adesione al trattamento sanitario proposto, rafforzando così la tutela del professionista.
- **Cartella infermieristica** (per professionisti infermieri): strumento raccomandato per registrare valutazioni, interventi assistenziali e monitoraggio dell'evoluzione clinica del paziente, garantendo continuità e qualità dell'assistenza.

L'adozione e l'utilizzo corretto di questi strumenti non solo rispondono a requisiti legali e deontologici, ma rappresentano anche un presidio fondamentale per la tutela della relazione di cura e della responsabilità professionale.

CHECKLIST PRATICA PER IL CONSENSO INFORMATO

Prima di raccogliere il consenso:

Verifica l'identità della persona assistita o del rappresentante legale.
Accertati della capacità di intendere e di volere dell'assistito.
Prepara una comunicazione semplice e chiara, adatta al livello culturale e linguistico della persona.
Prevedi il tempo necessario per spiegazioni e domande.

Durante l'informazione:

Descrivi la diagnosi o la situazione clinica attuale.
Illustra i trattamenti proposti, indicando benefici e rischi prevedibili.
Esplicita le alternative possibili, compreso il rifiuto o la rinuncia ai trattamenti.
Rispetta la volontà dell'assistito di ricevere ulteriori dettagli o approfondimenti.
Evita linguaggio tecnico incomprensibile o formule standardizzate.

Raccogliendo il consenso:

Ottieni una manifestazione di volontà esplicita: scritta o verbalizzata alla presenza di testimoni, se necessario.
Specificare il tipo di prestazione/assistenza a cui il consenso si riferisce.
Indica la possibilità di revoca del consenso in ogni momento.
Documenta l'avvenuta informazione e il consenso ottenuto (preferibilmente in forma scritta).
Se firma un rappresentante legale, annota chiaramente il ruolo (es. genitore, tutore, amministratore di sostegno).

Dopo la raccolta del consenso:

Archivia la documentazione in modo sicuro e conforme al GDPR.
Aggiorna il consenso se il piano assistenziale cambia in modo significativo.
Rispetta il diritto dell'assistito a modificare o revocare il consenso in qualsiasi fase dell'assistenza.

Particolare attenzione:

- Se la persona assistita appartiene a culture diverse, adatta l'informazione tenendo conto di valori, credenze e modelli di salute differenti.
- Se emergono dubbi sulla comprensione o sulla volontà dell'assistito, sospendere la procedura e approfondire.

Nota Bene:
Questa checklist rappresenta uno strumento di supporto pratico e non sostituisce l'obbligo deontologico e giuridico di una comunicazione personalizzata, rispettosa e continuativa.

FAC-SIMILE CONSENSO INFORMATO

In ambito sanitario, il consenso per ritenersi valido deve essere:

- Personale: indica che non è ammessa la rappresentanza di terzi (eccetto per i minori e per gli interdetti);
- Informato ed esplicito: è obbligo del professionista sanitario verificare la piena efficacia dell'informazione data all'assistito, che deve essere adattata alla piena capacità di comprensione dello stesso;
- Preventivo: va acquisito prima dell'esecuzione delle prestazioni richieste;
- Specifico: da parte dell'operatore, il quale ha il dovere di fornire tutti gli elementi necessari perché le caratteristiche del consenso siano tutte rispettate;
- Libero: deve essere ottenuto senza coercizioni di sorta, basato sulla valutazione dell'informazione, sulle possibili conseguenze di trattamento e di non trattamento e di alternative tra cure possibili;
- Consapevole: deve essere frutto di una scelta non condizionata o vincolata, senza errori o inganni, libero da coartazione, dalla dipendenza terapeutica e dalla supremazia del professionista
- Completo: va acquisito per tutte le prestazioni previste e/o per tutte le prestazioni che concorrono alla definizione del servizio per il quale si richiede il consenso;
- Attuale: l'intervallo di tempo tra la manifestazione del consenso e l'attuazione della prestazione deve essere breve, in modo da non far sorgere dubbi sulla persistenza della volontà dell'utente a sottoporsi al trattamento. Non deve essere considerato a tempo indeterminato;
- Manifesto: va acquisito con passi chiari e precisi e non è sufficienza l'assenza di dissenso o la presenza di un tacito consenso, né può essere ritenuto implicito;
- Revocabile: il consenso può essere revocato in qualsiasi momento, anche nell'immediatezza della procedura sanitaria che si sta ponendo in essere. L'assistito può esplicitamente rinunciare al diritto di essere informato: si parla in tal caso di assenso, ovvero quando siamo in una sorta di accettazione passiva alla proposta di cura; Recettizio: l'atto, essendo diretto a una persona determinata, produce effetti solo dal momento in cui perviene a conoscenza della persona a cui è destinato;
- Richiesto: l'esecuzione delle prestazioni e dei servizi richiesti è subordinata dalla raccolta in forma scritta e vincolata dalla presenza delle precedenti caratteristiche descritte.

Deve essere espresso da una persona capace, in possesso della capacità di intendere e di volere. Per quanto riguarda le persone interdette, l'informazione viene resa e l'espressione del consenso viene espressa dal tutore o dall'amministratore di sostegno con specifiche attribuzioni sulla sfera della salute. Le persone inabilitate possono essere autonome nel l'esprimere o meno il loro consenso.

Le persone incapaci naturali infine sono quei soggetti che, pur se non interdetti, si trovano per qualsiasi causa in condizioni tali da non essere in grado di dare un consenso o esprimere un dissenso.

Molta attenzione bisogna porre nel modo in cui vengono fornite le informazioni che devono essere chiare e comprensibili per l'utente, bisognerà quindi evitare di usare un linguaggio troppo professionale.

IL Dott. _ garantisce di attenersi scrupolosamente al rispetto di quanto sopra.

Pertanto, le prestazioni sanitarie e terapeutiche saranno erogate solo con il consenso informato dell'assistito (o del famigliare di riferimento o dell'amministratore di sostegno). Il consenso espresso nella parte sottostante può revocare il consenso espresso in precedenza.

Modulo di Consenso Informato per Progetto Assistenziale Personalizzato

Professionista sanitario: _____
Assistito: Cognome _____ Nome _____
Data di nascita: //_____ **Codice fiscale**: _____

INFORMAZIONE SULL'INTERVENTO ASSISTENZIALE
Il/la sottoscritto/a professionista ha informato il/la Sig./Sig.ra _____
in merito al progetto assistenziale personalizzato, che prevede:

- **Finalità**: migliorare, mantenere o ripristinare lo stato di salute e benessere della persona assistita attraverso interventi assistenziali pianificati e individualizzati.
- **Tipologie di prestazioni previste**: (es. medicazioni, gestione della terapia farmacologica, assistenza alla mobilizzazione, rilevazione dei parametri vitali, supporto educativo e motivazionale, attività di prevenzione delle complicanze).
- **Modalità di esecuzione**: interventi a domicilio / in sede ambulatoriale, secondo il piano definito con la persona assistita.
- **Durata prevista**: _____
- **Rischi e complicanze potenziali**: rischio di insuccesso parziale degli interventi, insorgenza di complicanze correlate allo stato di salute o ai trattamenti assistenziali.
- **Alternative possibili**: ricorso ad altri servizi sanitari pubblici o privati; possibilità di rifiutare singoli interventi.
- **Diritto di revoca**: la persona assistita può revocare il consenso al progetto assistenziale in qualsiasi momento senza necessità di motivazione.

DICHIARAZIONE DI CONSENSO
Il/la sottoscritto/a _____

- Dichiara di aver ricevuto informazioni complete, comprensibili e adeguate riguardo al progetto assistenziale proposto;
- Afferma di essere stato/a messo/a nelle condizioni di porre domande e di ricevere risposte chiare e soddisfacenti;
- Dichiara di aver compreso le finalità, le modalità, i benefici, i rischi e le alternative disponibili;
- Presta il proprio consenso libero e consapevole all'esecuzione del progetto assistenziale, autorizzando il professionista sanitario sopra indicato a realizzare le attività pianificate.

Luogo e data: _____
Firma dell'assistito (o di chi ne esercita la rappresentanza legale)

_____

Firma del professionista sanitario

_____

NOTA IMPORTANTE:

- In caso di rappresentanza legale, occorre allegare copia della documentazione che attesta la titolarità (es. procura, nomina di tutore o amministratore di sostegno).
- La persona assistita ha diritto di ricevere copia del presente modulo, unitamente al piano assistenziale condiviso

CONSENSO AL TRATTAMENTO DI RIPRESE FOTOGRAFICHE PER FINALITÀ SANITARIE

DATI ANAGRAFICI DEL PAZIENTE
Cognome: _____
Nome: _____
Questa sezione è da compilare a cura di:
☐ Paziente
☐ Genitore
☐ Tutore
☐ Amministratore di sostegno
☐ Persona di fiducia (in caso selezionare e compilare delega sottostante)
In merito alla possibilità che, nel corso di procedure terapeutiche, vengano eseguite **riprese fotografiche** della lesione trattata, da utilizzarsi **esclusivamente a fini clinici e assistenziali** per monitorare l'evoluzione della lesione da decubito e prevenire eventuali complicanze infettive (come infezioni batteriche):
DICHIARA CHE
☐ Acconsente liberamente e consapevolmente all'esecuzione delle riprese fotografiche, secondo le linee guida e le buone pratiche cliniche.
☐ NON acconsente all'esecuzione delle riprese fotografiche.
INOLTRE DICHIARA
Nel caso in cui non sia in grado di prestare direttamente il consenso, **delega** la seguente persona di fiducia:
Cognome: _____
Nome: _____
Tipo documento: _____
Numero documento: _____

FIRME
Firma del paziente/assistito: _____

Firma per consenso (se diverso dal paziente): _____

Data: _____ **Ora:** _____

Firma del delegato (se presente): _____

Firma del professionista: _____

Nota Bene: Il consenso può essere **revocato in qualsiasi momento**, semplicemente comunicandolo al personale sanitario di ELITE MEDICA LATINA SRL, che provvederà a interrompere l'utilizzo delle immagini e aggiornerà la documentazione.

7. NORMATIVA IN MATERIA DI PRIVACY

IL QUADRO NORMATIVO

Il Regolamento Generale sulla Protezione dei Dati (General Data Protection Regulation UE 2016/679, di seguito "GDPR"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, abroga la direttiva 95/46/CE, così creando un quadro normativo uniforme per tutti gli Stati membri dell'UE. Approvato nel maggio 2016, il GDPR è pienamente vigente dal 25 maggio 2018.
Con il Decreto legislativo n. 101 del 10 agosto 2018, l'ordinamento italiano ha recepito ufficialmente le disposizioni del GDPR, introducendo modifiche al Codice Privacy.
Si precisa che il Codice Privacy (D.Lgs. n. 196/2003) non è stato in toto abrogato bensì modificato ed integrato con il GDPR, a partire dal titolo che recita: «Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.»

DEFINIZIONI E PRINCIPALI RUOLI

Si riportano nella seguente tabella le principali definizioni contenute nell'art. 4 del GDPR, utili per la lettura del presente capitolo dedicato alla normativa in materia di protezione dei dati personali.

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.
DATI RELATIVI ALLA SALUTE	dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelino informazioni relative al suo stato di salute.
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.
TITOLARE	Titolare del trattamento: è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
RESPONSABILE	Responsabile del trattamento: è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

DPO	Responsabile per la protezione dei dati' (RPD, in inglese: 'Data Protection Officer', DPO): è un soggetto con competenze giuridiche qualificate, avente il compito di garantire l'osservanza del GDPR all'interno dell'azienda in cui opera attraverso attività di informazione, consulenza e indirizzo, agendo in contatto diretto con i vertici ma in modo indipendente. I Titolari e/o Responsabili di trattamento sono obbligati a nominare un RPD in determinati casi, tra i quali si evidenzia quello dell'esercizio, come attività principale, del monitoraggio regolare, sistematico e su larga scala delle persone fisiche; questa ipotesi infatti ricomprende 'tutte le forme di tracciamento e profilazione su Internet', nonché le 'attività di marketing basate sull'analisi dei dati raccolti'
INTERESSATO	la persona fisica cui si riferiscono i Dati Personali.

IL LIBERO PROFESSIONISTA QUALE TITOLARE DEL TRATTAMENTO

Il libero professionista (persona fisica) sarà titolare del trattamento di tutti i dati personali che vengono allo stesso forniti dai suoi clienti/pazienti. Nel caso invece di esercizio in forma associata sarà l'ente (studio associato, STP o cooperativa), in nome del legale rappresentante – ad essere qualificato Titolare del trattamento.

In base all'art. 5 del GDPR, i dati personali sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato (liceità, correttezza e trasparenza);
- 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 (limitazione della finalità);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
- 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 (esattezza);
- 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 presente GDPR a tutela dei diritti e delle libertà dell'Interessato (limitazione della conservazione);
- 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 (integrità e riservatezza);
- il Titolare del trattamento è competente per il rispetto dei principi e in grado di comprovarlo (responsabilizzazione).

Coloro che trattano dati personali devono rispettare tutti questi principi (ed essere in grado di dimostrarlo). Si rimarca, inoltre, che ai sensi dell'art. 24 del GDPR "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario" (c.d. principio dell'Accountability). Si tratta di una importante novità per la protezione dei dati in quanto si passa da una serie di

adempimenti imposti espressamente dalla normativa nazionale (quali, ad esempio, le “misure minime” contenute nell’Allegato B del Codice Privacy) ad un approccio più discrezionale che consente al titolare del trattamento di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel GDPR. Una maggiore autonomia bilanciata però, dall’onere di dimostrare come e per quali motivi sono state adottate determinate decisioni.
Pertanto, il libero professionista che esercita un’attività di natura libero-professionale deve garantire la conformità dei trattamenti eseguiti (sia da lui stesso in qualità di titolare che dai soggetti da lui eventualmente nominati come responsabili del trattamento) tramite l’adozione di procedure di trattamento adeguate e che possano rappresentare una prova documentale idonea a dimostrare la conformità del trattamento dei dati alla normativa in materia di protezione dei dati personali.

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento devono tener un registro delle operazioni di trattamento i cui contenuti sono indicati nell’art. 30 del GDPR (finalità del trattamento, descrizione delle categorie di Interessati e di dati personali trattati, termini ultimi previsti per la cancellazione dei dati, descrizione generale delle misure di sicurezza, ecc.).
L’obbligo di tenuta del registro non incombe sulle imprese o organizzazioni con meno di 250 dipendenti “a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all’articolo 9, paragrafo 1 (ndr: dati personali che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), o i dati personali relativi a condanne penali e a reati di cui all'articolo 10” (si veda, art. 30 paragrafo 5, del GDPR).
Tenuto conto che il libero- professionista tratta categorie particolari di dati di cui all’art. 9 del GDPR, esso dovrà tenere un registro delle attività di trattamento.
Il registro deve avere forma scritta, anche elettronica.
I contenuti del registro sono fissati, come suddetto, nell´art. 30 del GDPR; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell’ottica della complessiva valutazione di impatto dei trattamenti svolti.
Data Protection Impact Assessment (Valutazione d’impatto sulla protezione dei dati): quando un tipo di trattamento, allorché prevede in particolare l’uso di nuove tecnologie, considerati la natura, l’oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.
Il GDPR disciplina nel dettaglio il contenuto della valutazione d’impatto, prescrivendo al Titolare di coinvolgere il Responsabile della Protezione dei Dati (“RPD” o Data Protection Officer - DPO) nell’effettuazione della stessa; laddove la valutazione indichi che il trattamento presenterebbe un rischio elevato in assenza di misure volte ad attenuarlo, il Titolare prima di procedere al trattamento deve consultare l’Autorità di controllo (Consultazione preventiva, art. 36 del GDPR).

INFORMATIVA E CONSENSO

In caso di raccolta presso l’interessato, il Titolare del trattamento deve fornire, nel momento in cui i dati personali sono ottenuti, determinate informazioni specificatamente indicate nell’art. 13 del GDPR: tra queste si segnalano quella inerenti il periodo di conservazione dei dati (oppure, se non è possibile, i criteri per determinarlo) e quella riguardante il diritto dell’Interessato di revocare il consenso, ove previsto, in ogni momento.
Nel caso in cui il Titolare del trattamento intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'Interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente. Qualora i dati non siano raccolti presso l’Interessato, il Titolare deve fornire al medesimo anche l’indicazione della fonte da cui hanno origine i dati personali (art. 14 del GDPR).
Il consenso dell’Interessato (art. 7 del GDPR) è una delle condizioni di liceità del trattamento (art. 6, paragrafo 1, lett. a del GDPR).
Per “consenso dell'Interessato” si intende 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 (art. 4, n. 11, GDPR).
Il Titolare del trattamento deve essere in grado di dimostrare che l'Interessato ha prestato il proprio consenso (art. 7, paragrafo 1, GDPR). Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante (art. 7, paragrafo 2, GDPR).
L'Interessato ha il diritto di revocare il proprio consenso in qualsiasi momento, ciò non pregiudicando la liceità del trattamento basata sul consenso prima della revoca; il consenso deve poter essere revocato con la stessa facilità con cui è accordato (art. 7, paragrafo 3, GDPR). Il trattamento è legittimo anche in assenza del consenso dell'Interessato, purché sussista un'altra delle condizioni di liceità (art. 6 del GDPR), come ad esempio quando il trattamento sia necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, oppure quando esso sia necessario per adempiere un obbligo legale al quale è soggetto il Titolare, o ancora in presenza di un legittimo interesse del Titolare stesso che non prevalga sui diritti degli interessati.

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI.

Il libero professionista in sanità potrebbe dover trattare categorie particolari di dati personali in grado di rivelare "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"
In tal caso, occorre fare espresso riferimento a quanto sancito nell'articolo 9 del GDPR il quale prevede, al paragrafo 1, un divieto generale relativo trattamento di categorie particolari di dati personali.
Detto divieto non si applica se si verifica uno dei seguenti casi rilevanti per la prestazione in esame:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
oppure se:
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

DIRITTI DELL'INTERESSATO

DIRITTO DI ACCESSO (art. 15 GDPR)	l'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e a determinate informazioni specificamente indicate (finalità del trattamento, destinatari o categorie di destinatari cui i dati sono o saranno comunicati, periodo di conservazione dei dati, diritti dell'interessato, esistenza di un processo decisionale automatizzato, compresa la profilazione, ecc.).
DIRITTO DI RETTIFICA (art.16)	l'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il

	diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa
DIRITTO ALLA CANCELLAZIONE – DIRITTO ALL'OBLIO (art.17 GDPR)	n determinati casi (es. revoca del consenso, trattamento illecito, trattamento non più necessario etc...) l'Interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo.
DIRITTO DI LIMITAZIONE DEL TRATTAMENTO (art. 18 GDPR)	in determinati casi (es. contestazione dell'esattezza dei dati etc...) l'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento (alla sola operazione di conservazione dei dati personali).
DIRITTO ALLA PORTABILITA' DEI DATI (art.20 GDPR)	qualora il trattamento si basi su consenso o su contratto e sia effettuato con mezzi automatizzati, l'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati ad altro Titolare senza impedimenti da parte del primo.
DIRITTO DI OPPOSIZIONE (art.21 GDPR)	l'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, compresa la profilazione.
PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE, COMPRESA LA PROFILAZIONE (ART. 22 GDPR)	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. Tra le deroghe previste si ha il caso in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e il Titolare del trattamento o quello in cui la decisione si basi sul consenso esplicito dell'Interessato.

DATA BREACH

In base all'art. 32 il Titolare e il Responsabile, 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, mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; il GDPR indica in via esemplificativa alcune misure di questo tipo, tra le quali si citano:

- la pseudonimizzazione e la cifratura dei dati personali; la pseudonimizzazione consiste nel trattamento dei dati personali in modo tale che gli stessi 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 non siano attribuiti a una persona fisica identificata o identificabile (art. 4 GDPR);
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In caso di violazione dei dati personali (c.d. Data Breach, 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 – art. 4 GDPR), il Titolare notifica la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.
Se la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo (art. 33, paragrafo 1, del GDPR).
La notifica deve avere il contenuto minimo di cui all'art. 33, paragrafo 3, del GDPR. Quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento, senza ingiustificato ritardo, deve comunicare la violazione anche all'Interessato (art. 34 del GDPR).

SANZIONI

Ogni Stato membro dispone che una o più autorità pubbliche indipendenti ("Autorità di controllo") siano incaricate di sorvegliare l'applicazione del GDPR (artt. 51-62 GDPR); le Autorità di controllo hanno ampi poteri investigativi e correttivi, incluso quello di imporre il divieto definitivo del trattamento illegittimo. Chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del trattamento (art. 82 GDPR).
Ogni Autorità di controllo, in relazione a violazioni del GDPR, ha il potere di infliggere sanzioni amministrative effettive, proporzionate e dissuasive (artt. 83-84 GDPR). L'ammontare delle sanzioni può arrivare fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente. I singoli Stati membri possono prevedere ulteriori tipologie di sanzioni (anche penali).
A tal riguardo, il decreto legislativo n. 101 del 10 agosto 2018 ha previsto le seguenti fattispecie di reato, alcune delle quali nuove:

- Art. 167 (Trattamento illecito di dati);
- Art. 167 -bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala);
- Art. 167 -ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala);
- Art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante).