MODELLO ORGANIZZATIVO PRIVACY

Regolamento UE 2016/679

ORDINE PROVINCIALE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DI MODENA

REV	Data revisione	Oggetto	Responsabile	Firma
01		Prima approvazione	Il Legale Rappresentante p.t.	

INDICE

Sommario

1 Parte Generale

1.1 Definizioni

Per completezza ed esaustività, si riporta l'elenco delle definizioni di cui all'articolo 4 del GDPR.
Ai fini del presente regolamento s'intende per:
1) ***«dato personale»***: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) ***«trattamento»***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
3) ***«limitazione di trattamento»***: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
4) ***«profilazione»***: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
5) ***«pseudonimizzazione»***: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
6) ***«archivio»***: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
7) ***«titolare del trattamento»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
8) ***«responsabile del trattamento»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
9) ***«destinatario»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.
10) ***«terzo»***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
11) ***«consenso dell'interessato»***: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
12) ***«violazione dei dati personali»***: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) ***«dati genetici»***: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
14) ***«dati biometrici»***: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
15) ***«dati relativi alla salute»***: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
16) ***«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 presente regolamento;
17) ***«rappresentante»***: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
18) ***«impresa»***: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
19) ***«gruppo imprenditoriale»***: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
20) ***«norme vincolanti d'impresa»***: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
21) ***«autorità di controllo»***: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
22) ***«autorità di controllo interessata»***: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;
23) ***«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; oppure 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;
24) ***«obiezione pertinente e motivata»***: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
25) ***«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;
26) ***«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.

***

Ai fini del presente documento si elencano le definizioni utili:
"Modello": il presente Modello Organizzativo Privacy;
"Registro Titolare del trattamento": il registro contenente le seguenti sezioni: Intestazione, Valutazione del rischio, Misure di sicurezza, Trattamenti, Responsabili del trattamento, Protocolli/ Informative per la protezione dei dati;
"Registri Protezione Dati": il registro contenente le seguenti sezioni: Intestazione, Ruoli per la protezione dei dati, Registro dei dispositivi, Incaricati, Registro degli eventi, Registro delle violazioni;
"Enisa": acronimo di *European Union Agency for Network and Information Security*: si tratta di una delle più importanti ed affermate realtà in ambito Network e Information Security che pubblica mensilmente una serie di studi, report e indicazioni operative per la corretta applicazione delle metodologie di sicurezza secondo le normative vigenti in Europa;
"Gruppo di lavoro WP 29": **ovvero il** Gruppo dell'articolo 29 per la tutela dei dati (*Article 29 Working Party* o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati.
Era un organismo consultivo indipendente, composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione. Il Gruppo adottava le sue decisioni a maggioranza semplice dei rappresentanti delle autorità di controllo. Dal 25 maggio 2018 è stato sostituito dal Consiglio europeo per la protezione dei dati (EDPB) ai sensi del regolamento generale sulla protezione dei dati dell'UE (GDPR).
"CNIL": La Commission nationale de l'informatique et des libertés è un'autorità amministrativa indipendente francese incaricata di assicurare l'applicazione della legge sulla tutela dei dati personali nei casi in cui si effettuino raccolte, archiviazioni ed elaborazioni di dati personali.

1.2 Documenti utilizzati per la redazione del presente Modello

- The CNIL's Guide, 2018 Edition, Security of Personal Data;
- Enisa, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013;
- Enisa, Guidelines for SMEs on the security of personal data processing, December 2016;
- Enisa, Handbook on Security of Personal Data Processing, December 2017;
- Garante Privacy, Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – 7 marzo 2019 – doc. Web n. 9091942 – Registro dei provvedimenti n. 55 del 7 marzo 2019 -
- Garante Privacy, Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali – APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI, https://www.garanteprivacy.it/web/guest/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili;
- Gruppo di Lavoro WP29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", adottato il 16 febbraio 2010;
- Working Party 29 Position Paper on the derogations from the obligations to maintain records of processing activities pursuant to Article 30(5) GDPR;
- Gruppo di Lavoro WP29, Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017, Gruppo di lavoro articolo 29 per la protezione dei dati;
- Gruppo di Lavoro WP29, Linee Guida sui responsabili della protezione dei dati, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017;
- Gruppo di Lavoro WP29, Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 3 ottobre 2017;
- Gruppo di lavoro WP29, Guidelines on Automated individual decisione-making and Profiling for the purposes of Regulation 2016/679, adottare il 3 ottobre 2018, riviste e adottate il 6 febbraio 2018.

2 Introduzione normativa

Il Regolamento (UE) 2016/679 (di seguito GDPR, General Data Protection Regulation) 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, abroga la direttiva 95/46/CE, introducendo nuove regole organizzative per il corretto trattamento dei dati personali, definendo sanzioni commisurate al fatturato delle aziende e creando meccanismi di tracciabilità che impongono alle aziende di allocare al loro interno le responsabilità nel trattamento dei dati.
Il Regolamento è stato recepito nell'ordinamento italiano dal D.lgs. 10 agosto 2018, n. 101, che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196).
I destinatari sono tutti quei soggetti, anche extra europei, che sono chiamati a trattare in maniera automatizzata o meno i dati personali relativi a persone fisiche, siano essi clienti, dipendenti, utenti e fornitori.
Fermo restando che le novità più rilevanti verranno trattate nel prosieguo, si può ritenere che la vera rivoluzione copernicana consista nella responsabilizzazione del Titolare del Trattamento.
Il GDPR infatti non è un regolamento precettivo, che impone l'adozione di specifiche misure di salvaguardia dei dati personali uguali per tutti, ma lascia libero il Titolare del Trattamento di valutare la propria situazione e di predisporre un sistema idoneo per la salvaguardia dei dati personali trattati.
Ecco che la capacità di valutare con competenza la propria struttura organizzativa, tecnica ed informatica, costituisce il fulcro della riforma assieme alla capacità di dimostrare, in un'eventuale fase di controllo, le motivazioni a sostegno delle scelte effettuate.
In sostanza siamo di fronte ad un imponente cambiamento sul trattamento dei dati che vede il passaggio da un mero adempimento formale e burocratico ad un vero e proprio procedimento aziendale, che si inserisce nell'organizzazione interna di ogni realtà imprenditoriale privata e pubblica, e che, come si vedrà in seguito, dovrà garantire la protezione dei dati sin dalla fase dell'ideazione e della progettazione del prodotto o del servizio, sviluppando comportamenti in grado di prevenire ogni problematica inerente i dati personali.
Oltre al consenso dell'interessato quale base giuridica del trattamento, salvo i casi previsti dal legislatore, e l'obbligo di fornire adeguata informativa nei confronti dell'Interessato, le novità introdotte dal nuovo GDPR possono essere così riassunte:

- L'ambito di applicazione;
- Il principio di accountability;
- Data Protection Impact Assessment;
- Data Protection Officer;
- Il Registro delle operazioni di trattamento;
- Data Breach.

2.1. L'ambito di applicazione

Con il nuovo Regolamento viene introdotto il principio di applicazione del diritto dell'Unione Europea anche ai trattamenti di dati personali non svolti nell'Unione Europea, se relativi all'offerta di beni o servizi a cittadini UE o tali da comportare il monitoraggio dei loro comportamenti.
Nella Società odierna i sistemi di comunicazione tra le persone, le modalità di acquisto on-line, gli oggetti interconnessi, internet in generale, costituiscono il modo in cui tutti noi viviamo. Ne deriva che vengono trattati e gestiti una quantità indefinita di dati: sono proprio i dati e le informazioni a costituire uno degli asset maggiormente significativi per le imprese. Il regolamento si applica pertanto nei confronti di chiunque tratta dati personali di persone fisiche nello svolgimento della propria attività imprenditoriale e/o professionale, dovendo necessariamente porre l'attenzione anche ai sistemi digitali utilizzati per il trattamento degli stessi, ma non solo, dovendo esso applicarsi anche ai trattamenti effettuati senza l'ausilio di sistemi informatici, ipotesi oramai solo marginale e teorica visto il progresso tecnologico e l'era informatizzata in cui viviamo.
Se da un lato l'era digitale che viviamo permette a persone e a cose di essere interconnessi, dall'altro l'enorme quantità di dati e di informazioni impongono di porre attenzione alla loro salvaguardia nel rispetto dei principi fondamentali di ciascun individuo. È nell'alveo di questo contesto che il legislatore europeo ha emesso il GDPR.

L'obiettivo del GDPR è quello di consentire ai cittadini europei, ed a coloro che risiedono all'interno della UE, di poter confidare sul fatto che i propri dati personali siano trattati in maniera uniforme all'interno del territorio europeo.
In questo primo punto si vuole sottolineare un aspetto determinante: il legislatore europeo indica espressamente che il GDPR si applica ai Titolari del Trattamento o ai Responsabili del Trattamento che sono stabiliti all'interno dell'UE, anche se il trattamento dei dati avviene al di fuori dell'UE. Il secondo criterio è quello dell'ubicazione dell'individuo cui si riferiscono i dati personali: se si trova all'interno dell'UE, il GDPR si applica nel caso in cui il trattamento dei dati riguardi l'offerta di beni o servizi, o nel caso in cui il trattamento dei dati riguardi il monitoraggio del comportamento dell'individuo all'interno dell'UE.
Rispetto al precedente assetto normativo, l'ambito di applicazione territoriale costituisce una novità rilevante, atteso che società straniere che vendono beni o servizi all'interno dell'UE anche tramite e-commerce, dovranno rispettare i dettami del GDPR.

a. Consenso dell'Interessato e informativa

Il trattamento dei dati personali da parte del Titolare del trattamento e del Responsabile del trattamento[1] può considerarsi lecito esclusivamente previo **consenso espresso** da parte dell'Interessato, intendendosi per Interessato la persona fisica identificata o identificabile cui si riferisce il dato personale oggetto del trattamento.
Ai sensi dell'articolo 6 GDPR, Il trattamento è lecito, in deroga al consenso espresso, quando:

- è necessario per l'esecuzione di un contratto di cui è parte l'Interessato ovvero per l'esecuzione di misure precontrattuali prese su richieste del medesimo (ad esempio per quanto riguarda gli adempimenti contabili e fiscali);
- avviene in adempimento di un obbligo di legge per il Titolare;
- è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
- è necessario per l'esecuzione di un interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare;
- è necessario per perseguire un interesse legittimo del Titolare 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.

Si evidenzia che quest'ultima lettera apre la possibilità al Titolare del trattamento di giustificare la sussistenza di un interesse legittimo a fondamento di un trattamento di dati personali. In altri termini, il Titolare potrà ritenere sussistente un interesse non codificato dal legislatore sulla base della propria auto-valutazione, fermo restando la necessità di dover poi dimostrare il ragionamento sotteso alla propria scelta.
Per "consenso dell'interessato" deve intendersi "*qualsiasi manifestazione di volontà libera, specifica e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati che lo riguardano siano oggetto di trattamento*" (art. 4 par. 2 n. 11).
Il consenso è considerato una condizione di liceità alla stregua di quelle previste dal legislatore e deve essere in tutti i casi libero, specifico, determinato e informato. Non è ammesso il consenso tacito o presunto (pertanto non sono ammesse caselle pre-spuntate su un modulo e non sono lecite le prassi mediante le quali il

1

Il rapporto tra il Titolare ed il Responsabile del trattamento deve essere definito mediante un contratto che disciplini le materie di cui all'articolo 28.3 GDPR, in particolare oggetto, durata, natura e finalità del trattamento, tipologia di dati trattati, categorie di Interessati ed obblighi e diritti del data controller.

Con il nuovo Regolamento il Responsabile del trattamento ha un ruolo nuovo e più ampio, in particolare svolge un ruolo di più stretta collaborazione con il Titolare del trattamento; assume maggiori rischi connessi ad una sua immediata e diretta responsabilità relativamente ai trattamenti a lui affidati; costituisce un diretto interlocutore sia per l'Interessato che per le Autorità di controllo; risponde dell'eventuale attività di terzi suoi fornitori dovendo garantire il rispetto dell'applicazione della normativa da parte di tali soggetti.

È compito del Responsabile trattare i dati personali eseguendo le istruzioni ricevute dal Titolare; assicurare che tutti coloro che trattano i dati personali su sue indicazioni si siano impegnati a rispettare i vincoli di riservatezza; implementare e mantenere tutte le misure tecniche e organizzative adeguate; cooperare con il Titolare del trattamento per la gestione delle richieste di diritto d'accesso e per gli altri obblighi imposti dal Regolamento; su richiesta del Titolare cancellare o restituire i dati personali al termine del trattamento; fornire al Titolare qualsiasi informazione necessaria per dimostrare il rispetto del Regolamento; prevedere la presenza del Data Protection Officer ove prescritto o in vista delle caratteristiche dei trattamenti effettuati.

È ammessa la nomina di un subresponsabile. Per avvalersi di un altro soggetto si richiede un'espressa e documentata autorizzazione da parte del Titolare del trattamento. Il Responsabile del trattamento è tenuto a garantire che il proprio sub-fornitore (che dovrà essere designato Responsabile del trattamento) sottoscriva un documento contenente chiari e dettagliati obblighi in ordine al rispetto della normativa privacy e garantire che farà fronte, manlevando il Titolare, ad eventuali inadempimenti imputabili ad attività od omissioni dei propri sub-fornitori.

consenso, ad esempio raccolto in modalità informatica, sia già preimpostato o indirettamente coartato, facendone una condizione per conseguire una determinata prestazione) e deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".
Il consenso non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili) considerato altresì che il Titolare deve essere in grado di dimostrare che l'Interessato ha prestato il consenso a uno specifico trattamento. Ai sensi dell'articolo 7 GDPR, infatti, *"il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali"*.
Il consenso dei minori è valido a partire dagli anni 16; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.
Il consenso può essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal Titolare sulla base del consenso rimarranno comunque legittimi. Per tale motivo, risulterà particolarmente utile dotarsi di un data-base che possa registrare i consensi prestati e la loro eventuale revoca, con indicazione del periodo temporale: ciò permette al Titolare di poter anche dimostrare in quale periodo l'Interessato aveva prestato il consenso e quando lo aveva revocato. Questo aspetto è utile sia nei confronti del medesimo Interessato che esercita i propri diritti, sia nei confronti dell'Autorità di Controllo, permettendo al Titolare di poter dimostrare, anche a posteriori, la legittimità dei trattamenti effettuati.
Il consenso prestato per il trattamento dei dati "sensibili" deve essere "esplicito"; lo stesso dicasi per il consenso circa le decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22 GDPR).
La sussistenza di una condizione di liceità del trattamento non esonera il Titolare del medesimo dal dovere di informare adeguatamente gli Interessati.
Ad ogni modo il consenso può essere prestato solo a fronte di **un'informativa** che, ai sensi dell'articolo 12 GDPR, deve necessariamente essere resa in forma **concisa, trasparente, intelligibile, facilmente accessibile e con un linguaggio semplice e chiaro**, in particolare nel caso di informazioni destinate specificamente ai minori.
Le informazioni devono essere fornite per iscritto o con altri mezzi, se del caso in formato elettronico.
Se richiesto dall'Interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'Interessato.
Le informazioni possono essere fornite in combinazione con icone standardizzate per dare un quadro d'insieme del trattamento (ma pur sempre unitamente alla informativa estesa) e se presentate elettronicamente devono essere leggibili a macchina. Tali icone dovranno essere identiche in tutta l'Unione Europea e saranno definite dalla Commissione Europea.
Nel caso in cui i dati personali siano raccolti direttamente presso l'Interessato, il Titolare fornisce l'informativa nel momento stesso in cui i dati sono ottenuti. Qualora, invece, la raccolta dei dati avvenga presso soggetti diversi, l'articolo 14 GDPR dispone che l'informativa venga fornita:
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'Interessato, al più tardi al momento della prima comunicazione all'Interessato;
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
L'obbligo di rendere l'informativa da parte del Titolare viene meno nei seguenti casi:

- Se e nella misura in cui l'Interessato disponga già delle informazioni;
- Se comunicare tali informazioni risulta impossibile o implica risorse sproporzionate;
- Se l'ottenimento o la divulgazione dei dati sono previsti dal diritto dell'UE o da quello degli Stati membri.

Il Titolare deve adottare **misure appropriate per fornire all'Interessato le informazioni relative al trattamento**, ossia:

- **identità e coordinate di contatto** del Titolare, del suo rappresentante e dell'eventuale Data Protection Officer (Responsabile della protezione dei dati) se applicabile (sulla figura del DPO si tornerà successivamente);
- **finalità e base giuridica del trattamento**, considerato che per considerarsi lecito il consenso al trattamento dei propri dati deve essere prestato dall'Interessato per l'esercizio di una o più specifiche finalità da parte del Titolare;

- **legittimi interessi** perseguiti dal Titolare o da terzi[2], nelle ipotesi di cui all'art. 6, par. 1, lett. f *(il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore");*
- gli eventuali **destinatari** o le **categorie di destinatari** dei dati personali;
- **eventuale intenzione del Titolare di trasferire i dati all'estero[3] e le garanzie applicate;**
- **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione;
- **diritto dell'interessato**[4] di ottenere **l'accesso** ai dati personali[5] (Art. 15) e la **rettifica** (Art. 16) o la **cancellazione** degli stessi (Art. 17 diritto all'oblio[6]), o la **limitazione** del trattamento che lo riguardano (Art. 18) o di **opporsi** al loro trattamento, oltre al diritto di **portabilità** dei dati (art. 20);

---

2 Il bilanciamento fra legittimo interesse del Titolare o del terzo e diritti e libertà dell'Interessato non spetta all'Autorità ma è compito dello stesso Titolare; si tratta di una delle principali espressioni del principio di responsabilizzazione. L'interesse legittimo del Titolare o del terzo, come nella vecchia disciplina, deve prevale sui diritti e libertà fondamentali dell'Interessato per costituire un valido fondamento di liceità.

3 Si fa riferimento al trasferimento di dati personali oggetto di trattamento o destinati a essere oggetto di un trattamento verso un paese terzo non appartenente all'Unione Europea. Nella definizione di trasferimento è compreso anche il trasferimento successivo di dati personali da un paese terzo non appartenente all'Unione Europea verso un altro paese terzo.

Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.

Come avveniva già con la vecchia normativa, in mancanza di un riconoscimento di adeguatezza da parte della Commissione Europea, i Titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti. In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'Interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali).

Il Regolamento ha confermato la vecchia disciplina per quanto riguarda i flussi di dati al di fuori dell'Unione Europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

i) adeguatezza del Paese Terzo riconosciuta tramite decisione della Commissione Europea;

ii) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (norme vincolanti d'impresa - Binding Corporate Rules per la circolazione dei dati all'interno dei gruppi di imprese multinazionali ed approvate dall'Autorità di controllo competente, clausole contrattuali modello – standard model clause - adottate dalla Commissione, clausole tipo adottate dalle Autorità / DPA nazionali ed approvate dalla Commissione);

Vi è la possibilità di realizzare un contratto ad hoc con apposite clausole che disciplini il trasferimento dei dati nel paese terzo o verso l'organizzazione internazionale, previa autorizzazione dell'autorità di controllo, o di adottare Codici di condotta che definiscono garanzie adeguate o Certificazioni, accompagnati da un impegno "vincolante ed esaustivo" da parte del Titolare o del Responsabile stabilito nel paese terzo (contratto o atto unilaterale).

iii) in assenza di ogni altro presupposto, ovvero in mancanza di una decisione di adeguatezza ex art. 45 GDPR o in assenza di garanzie adeguate ex art. 46 GDPR, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni e disciplinate dall'articolo 49 GDPR. Nello specifico: consenso esplicito e informato dei rischi, esecuzione di un contratto, contratto stipulato con terze parti da parte del Titolare ma comunque a favore dell'Interessato, importanti motivi di interesse pubblico, esercizio di un diritto per azione legale, interesse vitale dell'interessato o di altre persone, dato tratto da un pubblico registro che fornisce informazioni al pubblico e che può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, purché il registro sia tale secondo il diritto dell'Unione o degli Stati Membri, legittimo interesse del Titolare. Si precisa che, ai sensi dell'articolo 49.5 GDPR è facoltà dell'Unione o degli Stati Membri, con il proprio diritto, fissare limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale, qualora tale limite venga adottato per motivi di interesse pubblico e notificando alla Commissione l'esistenza di tali limiti. Le decisioni di adeguatezza emanate in base alla Direttiva CE/95/46 restano in vigore, a meno che non siano modificate o abrogate dalla Commissione Europea.

Per consultare l'elenco aggiornato si veda http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi

4 Il termine per la risposta all'Interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 in caso di particolare complessità; il Titolare deve comunque dare un riscontro all'Interessato entro 1 mese dalla richiesta. È compito del Titolare valutare la complessità e stabilire l'ammontare dell'eventuale contributo da richiedere all'Interessato, ma solo in caso di richieste infondate o eccessive anche ripetitive; in caso di richiesta di più copie ripetitive il Titolare deve tenere conto dei costi amministrativi sostenuti.

Il riscontro deve avvenire in forma scritta, può essere dato oralmente solo se su richiesta dell'Interessato. La risposta deve essere intellegibile, concisa, trasparente, facilmente accessibile e fornita con un linguaggio semplice e chiaro.

5 Il diritto di accesso con la nuova disciplina prevede in ogni caso il diritto per l'Interessato di ricevere una copia dei dati personali oggetto di trattamento.

I Titolari possono altresì consentire agli Interessati di consentire di consultare direttamente, da remoto, i propri dati personali (considerando 63)

6 Con il nuovo GDPR si configura un diritto alla cancellazione di tipo rafforzato e dal campo di applicazione più esteso, in quanto il Titolare del trattamento ha l'obbligo di informare della richiesta gli altri titolari che trattano i dati personali cancellati, compresi qualsiasi link, copia o riproduzione. Il diritto all'oblio deve essere garantito nei seguenti casi: se i dati sono trattati solo sulla base del consenso dell'Interessato; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti o altrimenti trattati; se i dati sono trattati illecitamente, se l'Interessato si oppone legittimamente al loro trattamento o se i dati devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il Titolare.

Il diritto all'oblio potrà essere limitato solo in alcuni casi specifici: per esempio, per garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria; per tutelare un interesse generale (ad esempio, la salute pubblica); oppure quando i dati, resi anonimi, sono necessari per la ricerca storica o per finalità statistiche o scientifiche.

- qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- diritto di proporre reclamo ad un'Autorità di Controllo;
- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la **profilazione**[7], con l'indicazione della **logica** di tali processi decisionali e le conseguenze previste per l'Interessato. L'Interessato in tal caso ha il diritto di essere informato dell'attività di profilazione, di conoscere le logiche applicate al trattamento quando questo possa originare conseguenze giuridiche sul suo status ovvero condurre a possibili situazioni discriminatorie (come esempio il rifiuto della concessione di un prestito o il rigetto di una candidatura on-line "automatizzato") e di revocare il consenso prestato alla profilazione con la conseguenze che il Titolare deve sospendere il trattamento salvo dimostrare un "legittimo interesse".

Nel caso di profilazione per finalità di marketing la revoca del consenso implica l'immediata cessazione di tali attività da parte del Titolare.
Qualora il Titolare intenda trattare i dati raccolti per un'ulteriore finalità, prima di tale trattamento deve fornire all'Interessato le informazioni in merito a tale finalità diversa nonché tutte le informazioni pertinenti (periodo di conservazione, diritti esercitabili, natura del conferimento, ecc.).

b. Trattamento di dati "particolari" e giudiziari

Avendo riguardo al trattamento di dati "particolari", di cui all'art. 9[8], il GDPR, dopo aver espresso il generale divieto di trattamento, introduce, al paragrafo 2, determinate condizioni di liceità[9].

---

7 Si veda il paragrafo 7, Definizioni, numero 4. È necessario per aversi profilazione che vi sia una attività di elaborazione "automatizzata" dei dati raccolti destinata a produrre un profilo dell'Interessato e che la profilazione abbia conseguenze giuridiche, ossia produca delle valutazioni adottate "esclusivamente" sulla base di un trattamento automatizzato.

Non costituisce attività di profilazione il solo "tracciamento" della navigazione web dell'Interessato ma le attività di analisi volte alla profilazione dell'utente, in particolare per prendere decisioni che lo riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

8 *Articolo 9 GDPR, Trattamento di particolari categorie di dati personali, ovvero dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o vita sessuale o all'orientamento sessuale della persona.*

9 *a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;*

b) 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, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) 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;

d) 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, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) 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 sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

Anche in questo caso, pertanto, il consenso deve avvenire o previo consenso espresso ed esplicito da parte dell'interessato, ovvero deve sussistere una delle cause richiamate in nota; in ogni caso deve essere fornita adeguata informativa nei confronti dell'interessato.
A riguardo, il Garante ha chiarito che le deroghe al generale divieto di trattare le cc.dd. "categorie particolari di dati , tra cui vi rientrano quelli sulla salute, sono riconducibili all'art. 9 GDPR e ai seguenti trattamenti:

a. **motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri** (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice;

b. **motivi di interesse pubblico nel settore della sanità pubblica**, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);

c. **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** (di seguito "finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza. Gli eventuali trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità (artt. 6 e 9, par. 2, del Regolamento).

Il Garante riporta quindi alcuni esempi che non rientrano nelle ipotesi sopra descritte e che richiedono il consenso esplicito dell'Interessato:

a. trattamenti connessi all'utilizzo di **App mediche**, attraverso le quali autonomi titolari raccolgono dati, anche sanitari dell'interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato possano avere accesso soggetti diversi dai professionisti sanitari o altri soggetti tenuti al segreto professionale;

b. trattamenti preordinati alla **fidelizzazione della client**ela, effettuati dalle farmacie attraverso programmi di accumulo punti, al fine di fruire di servizi o prestazioni accessorie, attinenti al settore farmaceutico-sanitario, aggiuntivi rispetto alle attività di assistenza farmaceutica tradizionalmente svolta dalle farmacie territoriali pubbliche e private nell'ambito del Servizio sanitario nazionale (SSN);

c. trattamenti effettuati in campo sanitario da **persone giuridiche private per finalità promozionali o commerciali** (es. promozioni su programmi di screening, contratto di fornitura di servizi amministrativi, come quelli alberghieri di degenza);

d. trattamenti effettuati da professionisti sanitari per **finalità commerciali o elettorali**;

e. trattamenti effettuati attraverso il **Fascicolo sanitario elettronico** (d.l. 18 ottobre 2012, n. 179, art. 12, comma 5) In tali casi, l'acquisizione del consenso, quale condizione di liceità del trattamento, è richiesta dalle disposizioni di settore, precedenti all'applicazione del Regolamento, il cui rispetto è ora espressamente previsto dall'art. 75 del Codice. Al riguardo, un'eventuale opera di rimeditazione normativa in ordine all'eliminazione della necessità di acquisire il consenso dell'interessato

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

all'alimentazione del Fascicolo, potrebbe essere ammissibile alla luce del nuovo quadro giuridico in materia di protezione dei dati.

Diverso è il caso della refertazione on line per il quale il consenso dell'interessato è richiesto dalle disposizioni di settore in relazione alle modalità di consegna del referto (Decreto del Presidente del Consiglio dei Ministri 8 agosto 2013, art. 5).

Il trattamento dei dati giudiziari, di cui all'articolo 10 GDPR, può avvenire alle stesse condizioni di liceità di cui all'articolo 6 par. 1 sopra trattate. Vi sono inoltre due condizioni di liceità ulteriori, tra loro alternative:

- Controllo dell'Autorità pubblica nello svolgimento del trattamento;
- Autorizzazione basata sul diritto dell'Unione o su un diritto nazionale, che preveda le necessarie garanzie per gli interessati.

Nel caso di registri completi delle condanne penali, si osserva soltanto la prima condizione.

c. Il principio di accountability

Il GDPR prevede il cd. principio di accountability (responsabilizzazione), ovvero il principio in virtù del quale il Titolare del Trattamento, nel rispetto dei principi di carattere generale, deve adottare tutte le misure tecniche e organizzative idonee ed adeguate a garantire che il trattamento dei dati dal medesimo effettuati avvenga secondo le disposizioni del GDPR. Oltre a questo, il Titolare del Trattamento deve anche poter dimostrare e rendere conto delle scelte effettuate.

Il GDPR recita infatti che il Titolare del trattamento, "***tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, (…) mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.***

Dette misure ***sono riesaminate e aggiornate qualora necessario.***

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di ***politiche*** *adeguate in materia di protezione dei dati da parte del titolare del trattamento"* (art. 24 GDPR).

Le misure tecniche ed organizzative devono essere pertanto adeguate all'attività svolta e ai tipi di dati trattati nonché alle modalità di trattamento stesso, rendendosi così necessaria un'adeguatezza rispetto al caso concreto, al fine di evitare l'adozione di misure tecniche ed organizzative insufficienti o sproporzionate all'attività effettivamente svolta.

Spetta quindi al Titolare del Trattamento la responsabilità della scelta delle finalità e dei mezzi del trattamento dei dati personali.

Per tale ragione, è opportuno che le procedure di trattamento dei dati personali siano documentate. Il Titolare del trattamento dovrà dare prova di aver posto in essere un apparato di misure che effettivamente sia in grado di proteggere i dati degli Interessati, evitando che questi siano sottratti o persi o che ne venga fatto un uso distorto rispetto alle finalità per la quale sono stati raccolti.

Al riguardo è necessario porre l'attenzione ai concetti di **Privacy by Design** e **Privacy by Default**.

Per analizzare il loro portato e le conseguenze pratiche della loro applicazione, bisogna per prima cosa esaminare, seppur rapidamente, il dato normativo.

L'art. 25 del GDPR, rubricato "**Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**", stabilisce:

"*1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del

trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo".
Grazie all'analisi del primo paragrafo, dell'art. 25 del GDPR, è possibile individuare chiaramente il contenuto sostanziale del concetto di Privacy by Design. Tale locuzione indica una regola assai importante: fin dal momento della progettazione del trattamento dei dati personali degli utenti, e non solo nel momento dell'esecuzione, il Titolare del Trattamento deve mettere in atto misure tecniche ed organizzative adeguate alla protezione dei dati personali che vorrà trattare.
Nella pratica le misure tecniche a cui si è fatto poc'anzi riferimento devono essere volte a:
- **Pseudonimizzare** i dati personali raccolti. Il GDPR stabilisce che i dati raccolti debbano essere conservati in un formato che non identifichi direttamente uno specifico individuo, a meno che non si utilizzino informazioni aggiuntive[10].
- **Minimizzare** i dati personali raccolti. Gli enti e le imprese che decidano di raccogliere e trattare i dati personali di un soggetto, nell'ambito di uno specifico progetto o di una determinata attività, devono provvedere a raccogliere solamente i dati personali pertinenti allo scopo del trattamento, e nondimeno devono utilizzarli limitatamente a quanto risulta necessario per il perseguimento di suddette finalità.
- **Garantire il rispetto dei principi di carattere generale**. Ci si riferisce in particolare ai principi di liceità, correttezza, e trasparenza del trattamento dei dati; nonché al principio di limitazione delle finalità dei dati secondo cui i dati devono essere raccolti per finalità determinate, esplicite e legittime, e utilizzati solamente nella misura di quanto strettamente necessario per il raggiungimento di tali scopi. E poi ancora, al principio di esattezza dei dati, secondo cui i dati devono essere sempre esatti e aggiornati. Eventuali inesattezze devono essere tempestivamente rettificate. Ed ancora, al principio della limitazione della conservazione, secondo cui dati devono essere conservati per il tempo necessario al raggiungimento delle finalità per le quali sono trattati. Infine, i dati personali devono essere trattati in modo da garantire un'adeguata sicurezza dei dati, preservando la loro integrità e riservatezza.
Avendo riguardo al concetto di **Privacy by Default,** da una seppur rapida analisi del secondo comma dell'art. 25 del GDPR emerge come tale principio stabilisca che, per **impostazione predefinita**, i Titolari del Trattamento dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste, e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento dei dati garantendo la non eccessività dei dati raccolti.
Di fatto, adeguarsi al principio di Privacy by Default significa che tutte le volte in cui un Interessato comunichi i propri dati ad un Responsabile del Trattamento, deve sempre esistere a monte un protocollo interno / **una procedura /linea guida interna** alla stessa che preveda e disciplini le modalità di acquisizione, trattamento, protezione ed eventuale comunicazione a soggetti terzi. Pertanto, il Titolare del Trattamento deve predisporre misure tecniche predefinite in grado di garantire il rispetto della normativa sul trattamento dei dati personali.
Tale principio deve guidare il Titolare del Trattamento, nell'individuazione della quantità dei dati personali raccolti, della portata del trattamento, del periodo di conservazione e dell'accessibilità ai dati.
L'articolo 32, sicurezza del trattamento, recita inoltre che "(t)*enendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto* ***misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio****, che comprendono, tra le altre, se del caso:*
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (data recovery)*;*

10 Per la definizione di pseudonimizzazione, si veda il paragrafo 7, n. 5).
Il Considerando 26 recita, inoltre, che: "*I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono ad una persona fisica identificata o identificabile o a dati resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato*".
Il Regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche e di ricerca.

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".
Come rilevato dal Garante della Privacy[11] le misure adottate **devono essere idonee a garantire un adeguato livello di sicurezza al rischio** e, *"(...) in questo senso, **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva ("tra le altre, se del caso).** Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure minime di sicurezza (...) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento".*
Si lascia aperta la possibilità di aderire a codici di condotta elaborati dalle associazioni di categoria od ottenere certificazioni volontarie sulla gestione del trattamento dei dati personali.
Quali sono, pertanto, gli obblighi cui è tenuto il Titolare del Trattamento? Tale domanda, presuppone una risposta caso per caso. Difatti, se è vero che ogni Titolare del trattamento deve approntare le misure tecniche, organizzative ed informatiche idonee per garantire un livello di sicurezza adeguato al rischio per i dati personali trattati, è necessario valutare la tipologia di dati trattati (comuni, particolari etc), le finalità e le modalità del trattamento. Ad esempio in caso di dati particolari, ovvero quelli definiti dal D.lgs. 196/03 quali dati sensibili, una misura idonea per garantire il livello di sicurezza potrebbe essere la cifratura. Nell'ipotesi di dati elaborati a seguito di profilazione degli utenti di un sito e-commerce, potrebbe essere necessario attivare delle procedure di pseudonimizzazione.
L'elenco potrebbe essere lungo ma ciò che interessa evidenziare in questa sede è che la corretta valutazione delle misure da implementare va affrontata caso per caso, mediante una corretta analisi del rischio.
L'analisi del rischio (risk assessment e gap analysis) è pertanto necessaria al fine di individuare l'assetto societario attuale (as is) rispetto all'assetto che l'azienda necessariamente deve adottare al fine di garantire un'effettiva compliance alla normativa vigente (to be). Su tale aspetto si tornerà esaminando il metodo operativo adottato per l'adozione del Modello Privacy e la valutazione del rischio effettuata e riportata al capitolo 2 del presente Modello.

d. Data Protection Impact Assessment

La valutazione dell'impatto dei trattamenti sulla protezione dei dati, secondo quanto riportato dal Gruppo WP29 per la protezione dei dati[12], "*(...) è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, una*

11 Garante Privacy, Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali – APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI, https://www.garanteprivacy.it/web/guest/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

12 Gruppo istituito ex art 29 della Direttiva 95/49. È un organismo consultivo indipendente composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno stato membro, dal GEDP (Garante Europeo della protezione dei dati) nonché da un rappresentante della Commissione.

valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità"[13].

Il Gruppo WP29 ha evidenziato che, "(i)*n linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati,* ***non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*** (articolo 35, paragrafo 1)."

Ai sensi dell'articolo 35 paragrafo 3 "(l)*a valutazione di impatto sulla protezione dei dati di cui al paragrafo 1*[14] *è richiesta in particolare nei casi seguenti:*

- *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
- *il 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; o*
- *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

Le Linee Guida affermano che *"(i)l semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei dati non siano soddisfatte non diminuisce tuttavia* ***l'obbligo generale****, cui i titolari del trattamento sono soggetti,* ***di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati****. In pratica, ciò significa che i titolari del trattamento* ***devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche"****.*

Infatti, "(c)*ome indicato dalle parole "in particolare" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati. Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati*".

In tal senso, il Gruppo di Lavoro WP29 ha fornito **nove criteri**[15] da seguire per valutare il rischio ed un

---

13 Linee Guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017, Gruppo di lavoro articolo 29 per la protezione dei dati.

14 Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

15
a) Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso.

b) Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. (…)

c) Monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico)

d) Dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio dati biometrici, informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. (…). Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

e) Trattamento di dati su larga scala: si veda quanto riportato successivamente sulla corretta interpretazione dell'articolo 37 GDPR;

elenco di ipotesi di attività[16] che, sebbene non ricomprese nell'elenco di cui all'articolo 35 paragrafo 3, necessitano comunque di una valutazione di impatto sulla protezione dei dati.
Le stesse Linee Guida evidenziano però che *"(p)er contro, un trattamento può corrispondere ai casi di cui sopra* [ndr., si riferisce agli esempi riportati in tabella, di cui sono stati richiamati i *cases study* di cui alla nota 16, o comunque alle attività che rientrano nei criteri di cui alla nota n. 15] *ed essere comunque considerato dal titolare del trattamento un trattamento tale da non "presentare un rischio elevato". In tali casi il titolare del trattamento deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i punti di vista del responsabile della protezione dei dati.*
Il Gruppo di Lavoro WP29 insiste sul fatto che la valutazione di impatto sulla protezione dei dati non è necessaria *"quando il trattamento non è tale da "presentare un rischio elevato" oppure qualora esista una valutazione d'impatto sulla protezione dei dati analoga, o qualora il trattamento sia stato autorizzato prima del maggio 2018 oppure abbia una base giuridica o sia incluso nell'elenco delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla* protezione dei dati".
Si evidenzia inoltre che, ai sensi dell'articolo 35 par. 4, è compito dell'Autorità di Controllo redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati, ai sensi dell'articolo 35 par. 4, e ha la facoltà di redigere altresì un elenco delle tipologie di trattamenti per i quali non è richiesta una valutazione di impatto (art. 35 par. 5)[17].

---

f) Creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;

g) Dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (…), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione special (..) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

h) Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi;

i) Quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

16 Si riporta l'esempio di **un'azienda che monitora sistematicamente le attività dei suoi dipendenti,** controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc., mediante un monitoraggio sistematico e l'utilizzo di dati riguardanti soggetti interessati vulnerabili. Tale tipo di attività, a parere del Gruppo di Lavoro WP29, necessita di una valutazione di impatto sulla protezione dei dati.

Si riportano anche i seguenti esempi che potrebbero necessitare di una valutazione d'impatto sulla protezione dei dati: un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero). L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade; il Titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe. La raccolta di dati pubblici dei media sociali per la creazione di profili. Un'istituzione che crea banche dati antifrode e di gestione del rating del credito a livello nazionale. Conservazione dei dati per finalità di archiviazione di dati sensibili personalizzati pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.

Si riportano i seguenti esempi che non necessiterebbero di una valutazione d'impatto sulla protezione dei dati: un trattamento di dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. Una rivista on line che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati. Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati dal proprio sito web.

17 Alla data di approvazione del presente documento, l'Autorità di controllo belga ha incluso, nei trattamenti per cui la valutazione di impatto deve ritenersi obbligatoria, le seguenti ipotesi:

- Trattamenti che utilizzano dati biometrici per l'identificazione univoca di persone in luogo pubblico o in luogo privato accessibile al pubblico;
- Quando i dati personali vengono raccolti da terzi per essere successivamente utilizzati ai fini della decisione di rifiutare o risolvere un determinato contratto di servizi con una persona fisica;
- Quando il trattamento riguarda categorie particolari di dati personali, ai sensi dell'articolo 9 GDPR, che sono utilizzati per uno scopo diverso da quello per il quale sono stati raccolti, tranne nel caso in cui il trattamento sia basato sul consenso dell'Interessato o se è necessario per adempiere ad un obbligo legale a cui è sottoposto il Titolare;
- Quando il trattamento viene eseguito utilizzando un apparato, ed una violazione dei dati personali potrebbe compromettere la valutazione fisica dell'Interessato;
- nel caso di trattamento su larga scala di dati personali di soggetti vulnerabili, compresi i bambini, per uno o più scopi diversi da quelli per i quali i dati sono stati raccolti;
- quando i dati vengono raccolti su larga scala da terze parti per analizzare o prevedere la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione o il movimento di persone fisiche;

Il Garante italiano è intervenuto individuando un elenco di tipologie di trattamenti che necessitano della valutazione di impatto sulla protezione dei dati[18], ovvero:

1. trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
2. trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi);
3. trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma

---

- quando particolari categorie di dati personali ai sensi dell'articolo 9 GDPR o dati di natura molto personale (come i dati sulla povertà, disoccupazione, partecipazione al lavoro giovanile o lavoro sociale, dati di attività domestiche e private, dati di localizzazione) sono sistematicamente scambiati tra diversi titolari;

- quando si tratta di elaborazione su larga scala di dati generati da dispositivi dotati di sensori che inviano dati via Internet o altri mezzi (Internet of Things, come smartTV, elettrodomestici intelligenti, giocattoli, smart cities, contatori intelligenti di energia, ecc.) e tale trattamento viene utilizzato per analizzare o prevedere la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione o il movimento delle persone fisiche;

- quando si tratta di elaborazione su larga scala e/o sistematica di dati di telefonia, Internet o altri dati di comunicazione, metadati o dati di localizzazione di persone fisiche o che consentano di condurre a persone fisiche (ad es. tracciamento wifi o elaborazione dei dati sulla posizione dei viaggiatori nel trasporto pubblico) quando il trattamento non è strettamente necessario per l'esecuzione di un servizio richiesto dall'interessato;
- in caso di elaborazione automatizzata e sistematica di dati personali su larga scala in cui il comportamento delle persone fisiche è monitorato, raccolto, stabilito o influenzato, inclusi i trattamenti per scopi pubblicitari.

Secondo l'Autorità belga, non è necessario effettuare la valutazione di impatto nei seguenti casi:

- i trattamenti effettuati da privati necessari ad adempiere ad un obbligo normativo, e per i quali la legge abbia indicato gli scopi dell'elaborazione, le categorie di dati personali e le garanzie per prevenire abusi o accessi o trasferimenti illegittimi;
- il trattamento relativo esclusivamente ai dati necessari per l'amministrazione degli stipendi dei dipendenti del Titolare, quando i dati sono utilizzati unicamente per tale finalità, sono comunicati solo ai destinatari autorizzati a tale scopo e non vengono conservati più a lungo del tempo necessario per conseguire la finalità del trattamento;
- il trattamento relativo esclusivamente all'amministrazione dei dipendenti del Titolare, nella misura in cui tale trattamento non coinvolge i dati relativi alla salute degli interessati o altre particolari categorie di dati di cui all'art. 9 GDPR o dati di cui all'art. 10 GDPR, ed i dati personali non vengono conservati più a lungo del tempo richiesto per la finalità di amministrazione del personale e sono comunicati a terzi solo se previsto da una disposizione di legge o regolamentare o per la realizzazione delle finalità del trattamento;
- trattamenti di dati personali che riguardano esclusivamente la contabilità del Titolare, quando i dati vengono utilizzati esclusivamente per tale finalità, e purché i dati personali non sono conservati più a lungo del tempo necessario al conseguimento delle finalità del trattamento ed i dati personali trattati sono comunicati a terzi in base ad una previsione di legge o la comunicazione è necessaria per la contabilità;
- il trattamento di dati personali relativi all'amministrazione di azionisti e soci quando il trattamento riguarda solo i dati necessari per tale amministrazione, e sono comunicati a terzi esclusivamente in base ad una previsione di legge o regolamentare e non vengono conservati oltre il tempo necessario per raggiungere gli scopi del trattamento;
- il trattamento di dati personali da parte di una fondazione, associazione o qualsiasi altra istituzione senza scopo di lucro in occasione delle sue attività abituali, a condizione che il trattamento riguardi esclusivamente i dati personali relativi ai propri membri, alle persone con cui il Titolare mantiene contatti regolari quali beneficiari, purché non vi siano dati ottenuti da terzi, e che i dati non vengano conservati più a lungo del tempo richiesto per l'amministrazione e siano comunicati a terzi solo in presenza di una disposizione di legge o regolamentare;
- il trattamento di dati personali relativo alla registrazione dei visitatori per il controllo accessi, quando i dati elaborati sono limitati al nome ed indirizzo professionale del visitatore, all'identificazione del suo datore di lavoro, all'identificazione del veicolo, al nome, la sezione e la funzione della persona visitata ed al momento della visita, ed i dati non sono conservati oltre il tempo necessario alla finalità di controllo accessi;
- il trattamento di dati personali da parte di istituti di formazione per la gestione dei loro rapporti con gli alunni e studenti, purché il trattamento si riferisca solo a studenti attuali e potenziali o ad ex studenti e non vengano trattati dati ottenuti da terzi, e la comunicazione avvenga unicamente sulla base di una disposizione normativa o regolamentare ed il dato non sia conservato per un periodo superiore a quello necessario a mantenere la comunicazione tra lo studente e l'istituto;
- il trattamento di dati personali relativi esclusivamente alla gestione dei clienti e fornitori del Titolare, purché il trattamento riguardi solo clienti e fornitori attuali o precedenti e non siano ricomprese particolari categorie di dati, ex art. 9 GDPR o dati di cui all'art. 10 GDPR, e per quanto riguarda l'amministrazione della clientela, non vengano registrati dati forniti da terzi, ed i dati siano conservati per il periodo necessario alla normale gestione della clientela del Titolare e siano comunicati a terzi solamente in base ad una norma di legge o di regolamento o nel quadro della normale gestione aziendale.

18 Elenco delle tipologie di trattamenti soggetti al requisito della valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 [9058979] - Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018 - Allegato 1, Elenco delle tipologie di trattamenti , soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.;

4. trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);
5. trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;
6. trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01;
8. trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
9. trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
10. trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse;
11. trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento;
12. trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

La valutazione di impatto non risulta pertanto necessaria nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo[19];

19 In questo senso, si specifica che una valutazione di impatto può riguardare non solo una singola operazione di trattamento dei dati ma anche trattamenti multipli e simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Il WP29, specifica a riguardo che "In effetti, le valutazioni d'impatto sulla protezione dei dati mirano a studiare sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le libertà delle persone fisiche e non è necessario realizzare una valutazione d'impatto sulla protezione dei dati nei casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalità specifica) che sono già stati studiati. Questo potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Ad esempio, un gruppo di autorità comunali che istituiscono ciascuna un sistema di televisione a circuito chiuso simile potrebbe svolgere una singola valutazione d'impatto sulla protezione dei dati che copra il trattamento svolto da tali titolari del trattamento distinti; oppure un gestore ferroviario (un titolare del trattamento unico) potrebbe esaminare la videosorveglianza in tutte le sue stazioni ferroviarie realizzando una singola valutazione d'impatto sulla protezione dei dati. Ciò può essere applicabile anche a trattamenti simili attuati da vari titolari del trattamento di dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile una valutazione d'impatto sulla protezione dei dati di riferimento, attuare le misure descritte nella stessa, e fornire una giustificazione per la realizzazione di una singola valutazione d'impatto sulla protezione dei dati".

Coerentemente a quanto appena riportato, il WP29 riporta l'esempio contrario, in cui comunque persiste l'obbligo di effettuare una PIA da parte del Titolare: "Una valutazione d'impatto sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento. Ovviamente, il titolare del trattamento che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria valutazione d'impatto sulla protezione dei dati in relazione all'attuazione specifica, tuttavia tale valutazione del titolare del trattamento può utilizzare le informazioni fornite da una valutazione analoga preparata dal fornitore del prodotto, se opportuno. Un esempio potrebbe essere rappresentato dalla relazione tra produttori di contatori intelligenti e società fornitrici di servizi pubblici. Ogni fornitore di prodotti o responsabile del trattamento dovrebbe condividere informazioni utili senza compromettere i segreti né generare rischi per la sicurezza, divulgando vulnerabilità".

- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate; in tal caso la valutazione d'impatto sulla protezione dei dati deve essere effettuata per le operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento;
- qualora un trattamento, necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, e tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10);
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5).

È bene evidenziare infine che la preventiva consultazione dell'Autorità di Controllo è necessaria, ai sensi dell'articolo 36, solo qualora valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati. Pertanto, solo in questo caso il Titolare del trattamento sarà tenuto a richiedere la consultazione preventiva dell'Autorità di Controllo in relazione al trattamento, fornendo la valutazione effettuata.

e. Data Protection Officer

Il nuovo Regolamento ha inoltre introdotto una nuova figura indipendente di controllo, il **Data Protection Officer (DPO)**, in italiano Responsabile Protezione Dati, figura autonoma e distinta dal Titolare e dal Responsabile del trattamento dati.

È un soggetto, interno o esterno alle organizzazioni (al riguardo è ammessa anche la sottoscrizione di un contratto di servizi), che deve avere un ruolo specifico e indipendente[2021], con competenze giuridiche, informatiche, di risk management e di analisi dei processi. Il grado di conoscenze specialistiche deve essere adeguato alla singola realtà aziendale, in quanto "*(...) non trova una definizione tassativa, piuttosto deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento*"[22]. Anche le qualità professionali non sono preventivamente individuate e specificate, ma il Gruppo di lavoro WP29, nelle Linee guida richiamate in nota, ritiene comunque necessaria una conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del GDPR, oltre che una formazione adeguata e continua. Si richiede inoltre una buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati.

È ammessa la nomina di un DPO unico per un gruppo imprenditoriale, a condizione che sia "facilmente raggiungibile da ciascuno stabilimento" (art. 37 par. 2 GDPR), considerato che il DPO deve essere un punto di contatto per interessati, autorità di controllo e soggetti interni all'organismo o all'ente.

La nomina del DPO non è obbligatoria, se non in determinati casi individuati dall'articolo 37 GDPR:

a) se il trattamento di dati personali è effettuato da un'autorità pubblica o da un organismo pubblico;
b) quando le attività principali dell'organizzazione consistono in trattamenti che richiedono il "monitoraggio regolare e sistematico" degli Interessati "su larga scala";
c) quando le attività principali dell'organizzazione consistono nel trattamento "su larga scala" di dati "sensibili" ("categorie particolari di dati") o "giudiziari" ("dati personali relativi a condanne penali e reati").

---

20 È necessario che il DPO soddisfi i requisiti di cui alla sezione IV del GDPR, che si trovi quindi in un'effettiva situazione di indipendenza, che riferisca direttamente al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento e che non si trovi in una situazione di conflitto di interessi nello svolgimento di altri compiti o funzioni. Non sono ammessi atti ritorsivi nei confronti del DPO per le funzioni svolte, ad esempio risoluzione ingiustificata del contratto di servizi.

21 Per garantire un'effettiva indipendenza è necessario assegnare al DPO le necessarie risorse, sia di tipo economico che fisico (mediante la composizione di un team di lavoro) oltre che strutturali, per assolvere ai propri compiti, accedere ai dati personali e ai trattamenti e per mantenere la propria competenza specialistica. Le risorse devono essere adeguate all'attività in concreto svolta, in quanto tanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del DPO.

22 Linee Guida sui responsabili della protezione dei dati, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017.

Nulla vieta alla Società di dotarsi di un DPO su base volontaria, in tal caso troveranno applicazione tutti i requisiti di cui agli articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del DPO esattamente come nel caso di una nomina obbligatoria.
Il Gruppo di Lavoro (WP29) nelle Linee Guida chiarisce l'obbligatorietà o meno del DPO in riferimento a quanto previsto dall'articolo 37.
Innanzitutto *"Il Gruppo di Lavoro raccomanda ai titolari del trattamento e responsabili del trattamento di* ***documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD*** (ndr DPO)*,* ***così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti. Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario, per esempio se i titolari del trattamento o i responsabili del trattamento intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'articolo 37, paragrafo 1".***
Ponendo l'attenzione alle lettere b) e c) del paragrafo 1 sopra citato, le Linee Guida forniscono un aiuto per la corretta interpretazione dei termini utilizzati.
Per attività principali (**core activities**) devono intendersi le attività principali e non accessorie, le operazioni necessarie al raggiungimento degli obiettivi prefissati dall'azienda, ma non deve essere comunque interpretata nel senso di escludere quei casi in cui il trattamento di dati, pur non costituendo attività principale, costituisce comunque una componente inscindibile dalle attività svolte.
Avendo riguardo al concetto di "**larga scala**", ai sensi del considerando 91, devono intendersi per "*trattamenti su larga scala*, (quei trattamenti) *che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*".
Il Gruppo di lavoro fornisce anche in questo caso dei fattori, dei criteri utili[23] al fine di stabilire se un trattamento debba considerarsi effettuato su larga scala.
Il monitoraggio, infine, per considerarsi **regolare**, deve avvenire almeno secondo una delle seguenti modalità:

- in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- in modo ricorrente o ripetuto a intervalli costanti;
- in modo costante o a intervalli periodici.

L'**aggettivo sistematico** deve possedere invece almeno uno dei seguenti significati:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Vengono fornite quindi alcuni esempi a titolo esemplificativo di attività che possono configurare un monitoraggio regolare e sistematico[24].
La responsabilità principale del DPO è quella di osservare, valutare e organizzare la gestione del trattamento dei dati personali (e dunque la loro protezione) all'interno di un'azienda affinché questi siano trattati nel rispetto delle normative.
Il considerando 97 del GDPR specifica che il Titolare del trattamento o il Responsabile del trattamento dovrebbe essere *"assistito [dal DPO] nel controllo del rispetto a livello interno del presente regolamento".*
Il DPO deve informare e consigliare il Titolare, il Responsabile o l'Incaricato e tutti coloro che trattano dati personali circa i loro obblighi, ai sensi del Regolamento e delle altre disposizioni dell'Unione o dello Stato membro in materia di protezione dei dati; controllare il rispetto del Regolamento, delle altre disposizioni relative alla protezione dei dati dell'Unione o dello Stato membro e delle regole del Titolare, del Responsabile o dell'Incaricato in materia di protezione dei dati personali, inclusi l'assegnazione delle

23 · il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; · il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; · la durata, ovvero la persistenza, dell'attività di trattamento; · la portata geografica dell'attività di trattamento.

24 curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi; fornire informazioni ove richiesto per quanto riguarda la valutazione d'impatto sulla protezione dei dati e monitorare i relativi adempimenti ai sensi dell'Articolo 33[25]; cooperare con l'autorità di vigilanza; agire come punto di contatto per l'autorità di vigilanza sulle questioni relative al trattamento dei dati personali, inclusa la consultazione preliminare di cui all'Articolo 34 in caso di comunicazione all'interessato per le violazioni dei dati personali (data breach), e fornire informazioni, se del caso, su qualsiasi altra questione. Inoltre il Responsabile della protezione dei dati deve, nell'esercizio dei propri compiti, prendere in debita considerazione i rischi associati alle operazioni di trattamento, avuto riguardo alla natura, allo scopo, al contesto e alle finalità del trattamento.
Le stesse capacità personali devono essere proporzionate agli stessi compiti che il DPO deve svolgere, in quanto ricopre *"(...) un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali*".
Si deve precisare inoltre che, come rilevato nelle Linee guida del Gruppo di lavoro WP29, "*il controllo del rispetto del regolamento non significa che il [DPO] sia personalmente responsabile in caso di inosservanza. Il [GDPR] chiarisce che spetta al titolare, e non al [DPO], "mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento" (articolo 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, e non del [DPO]*".

Avendo riguardo alle strutture sanitarie, il Garante ha chiarito che, in generale, si ritiene che i trattamenti dei dati personali relativi a pazienti effettuati da un'azienda sanitaria appartenente al SSN devono essere ricondotti a quelli per i quali è prevista la designazione obbligatoria del DPO, sia in relazione alla natura giuridica di "organismo pubblico" del titolare, sia in quanto rientrano nella condizione prevista dall'art. 37, par. 1, lett. c), considerato che le attività principali del titolare consistono nel trattamento, su larga scala, di dati sulla salute.

Anche il trattamento dei dati relativi a pazienti svolto da un ospedale privato, da una casa di cura o da una residenza sanitaria assistenziale (RSA) può rientrare, in linea generale, nel concetto di larga scala.

Anche per gli aspetti organizzativi dell'ufficio del DPO, la possibilità e la fattibilità (art. 39 del Regolamento) di nominare un unico DPO per più strutture sanitarie, è rimessa alla responsabilità del titolare del trattamento.

Quanto, poi, al singolo professionista sanitario che operi in regime di libera professione a titolo individuale, si fa presente che lo stesso non è tenuto alla designazione di tale figura con riferimento allo svolgimento della propria attività.

Secondo quanto indicato nel Considerando n. 91 del Regolamento, infatti, i trattamenti dallo stesso effettuati non rientrano tra quelli su larga scala. In tal senso, anche il Gruppo di lavoro Art. 29 per la protezione dei dati indica, tra gli esempi di trattamento da non considerare su larga scala, quelli svolti da un singolo professionista sanitario .

Analoghe considerazioni valgono anche per le farmacie, le parafarmacie, le aziende ortopediche e sanitarie. Pertanto, i citati soggetti, se non effettuano trattamenti di dati personali su larga scala, non sono obbligati a designare il DPO.

---

25 Nelle Linee Guida richiamate, "*il Gruppo di lavoro raccomanda che il titolare del trattamenti si consulti con il [DPO], fra l'altro sulle seguenti tematiche: se condurre o meno una [PIA]; quale metodologia adottare nel condurre una [PIA]; se condurre la [PIA] con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate; se la [PIA] sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al [GDPR]. Qualora il titolare del trattamento non concordi con le indicazioni fornite dal [GDPR], è necessario che la documentazione relativa alla [PIA] riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni*" Il WP29 raccomanda infine di disciplinare con apposito contratto il rapporto tra il Titolare e il DPO e fornendo indicazioni, mediante apposita informativa a dipendenti, amministratori e altri aventi causa, dei compiti assegnati al DPO.

f. Registro delle operazioni di trattamento

I Titolari e i Responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti[26], devono tenere un **registro delle operazioni di trattamento** che deve avere forma scritta o anche elettronica ed i cui contenuti sono indicati all'articolo 30 del GDPR. Al riguardo, il Garante per la Privacy lo definisce uno "***strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato di trattamenti in essere all'interno dell'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio***"[27].

Conclude il Garante sostenendo nelle raccomandazioni che **"(l)*a tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.*** *I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno nell'ottica della complessiva valutazione di impatto dei trattamenti svolti. Nello specifico, si richiama l'attenzione sulla sostanziale coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art 30 regolamento; l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i titolari potranno integrare nei modi opportuni".*

Ai sensi dell'articolo 30 GDPR, il Titolare del trattamento e, ove applicabile, il suo Rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.

Tale registro deve contenere tutte le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del Rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di Interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di dati acquisiti da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e che può essere consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse (art. 49 par. 2 GDPR), la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Ogni Responsabile del trattamento e, ove applicabile, il suo Rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento, contenente:

a) il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del Rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

I registri devono essere tenuti in forma scritta, anche in formato elettronico.

Su richiesta, il Titolare del trattamento o il Responsabile del trattamento e, ove applicabile, il Rappresentante del Titolare del trattamento o del Responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

---

26 salvo che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessati, il trattamento non sia occasionale o includa il trattamento di dati sensibili o giudiziari

27 Garante Privacy, Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili. https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

g. Il Responsabile del trattamento

Il Responsabile del trattamento dei dati è un soggetto esterno alla realtà aziendale che svolge, nell'interesse del Titolare, un trattamento dei dati personali.
Ai sensi dell'articolo 28 GDPR, "*qualora un trattamento debba essere svolto per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*". È pertanto onere dello stesso Titolare del trattamento assicurarsi che soggetti esterni, cui possono essere comunicati i dati o che possano venire a conoscenza dei dati trattati, assicurino le medesime misure tecniche ed organizzative necessarie, nel rispetto del principio di accountability.
I rapporti tra il Titolare e il Responsabile esterno del trattamento devono essere regolati da un contratto o un altro atto giuridico avente forza di legge, secondo il diritto dell'Unione o degli stati membri, stipulato in forma scritta anche in formato elettronico.
La nomina di Responsabile esterno del trattamento e i rapporti tra Titolare e Responsabile possono essere regolati direttamente dal contratto avente ad oggetto la prestazione del servizio ovvero da un contratto, parte integrante del primo e la cui efficacia è vincolata alla scadenza dello stesso. In tal caso la nomina di Responsabile esterno del trattamento perderebbe pertanto efficacia e si intenderebbe revocata senza esplicita comunicazione da parte del Titolare alla scadenza del primo contratto sottoscritto, salvo proroga anche tacita.
Il contratto o altro atto avente forza di legge, ai sensi del paragrafo 3 art. 28 GDPR, deve vincolare il Responsabile esterno al Titolare, stipulare la durata, la natura e la finalità del trattamento, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento. Nello specifico deve prevedere che il Responsabile:

- Tratti i dati solo su istruzione documentata del Titolare, anche in caso di trasferimento verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o il diritto nazionale cui è soggetto il Titolare del trattamento. In tal caso è onere del Responsabile darne avviso al Titolare prima dell'inizio del trattamento, salvo che tale diritto vieti il rilevamento di tale informazione per motivi di interesse pubblico;
- adotti le misure richieste dall'art. 32 del GDPR e, in generale, le misure tecniche e organizzative che risultano essere necessarie al fine di ridurre al minimo il rischio di distruzione e perdita, anche accidentali dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, per quanto di propria competenza. In particolare, il Responsabile deve consentire agli Interessati, ovvero ai soggetti cui si riferiscono i dati, di esercitare i diritti ad essi garantiti dal GDPR, informando tempestivamente il Titolare delle relative richieste, fornendo altresì copie delle risposte;
- su scelta del Titolare, cancelli o gli restituisca tutti i dati personali al termine della prestazione dei servizi relativa al trattamento e cancelli le copie esistenti, salvo che vi sia un obbligo di legge che ne preveda la conservazione;
- metta a disposizione del Titolare le informazioni necessarie per dimostrare il rispetto degli obblighi esplicati e disciplinati dall'articolo 28, e contribuisca alle attività di revisione o ispezione realizzate dal Titolare o da altro soggetto incaricato;
- comunichi al Titolare ogni violazione dei dati personali subita, senza ingiustificato. Al riguardo il legislatore non fornisce alcun termine. Il Gruppo WP 29[28] ha affermato che la comunicazione deve essere effettuata immediatamente, al fine di consentire al Titolare del trattamento di effettuare le verifiche del caso e di procedere con le notifiche, se necessario, nei confronti dell'autorità nel termine di 72 ore e degli Interessati senza ingiustificato ritardo;
- informi tempestivamente il Titolare di qualsiasi richiesta pervenuta da parte dell'Autorità Garante per la protezione dei dati personali e/o dall'Autorità giudiziaria.

Qualora il Responsabile esterno del trattamento intenda subappaltare, in tutto o in parte, le attività di cui al contratto sottoscritto o ad altro atto avente forza di legge, dovrà ottenere un preventivo consenso scritto da parte del Titolare. Ai fini della richiesta di consenso, il Responsabile deve indicare le attività oggetto di subappalto ed i soggetti ai quali intende affidare l'incarico.

28 Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 3 ottobre 2017.

Il Responsabile, all'esito dell'ottenimento del consenso da parte del Titolare, deve stipulare un contratto scritto con i subappaltatori che preveda il rispetto di quanto sopra esposto, provvedendo a nominarli sub-responsabili del Trattamento.
L'adesione del responsabile a codici di condotta o a un meccanismo di certificazione può essere utilizzata dal Titolare per dimostrare le garanzie richiamate.

h. Data Breach

La sezione 2 del GDPR, concernente la "sicurezza dei dati trattati", oltre a quanto già esaminato circa le misure tecniche e organizzative che il Titolare e il Responsabile del trattamento devono adottare per garantire un livello di sicurezza adeguato al rischio (art. 32 GDPR), ai successivi due articoli disciplina la gestione delle violazioni di sicurezza dei dati personali.
La definizione di data breach la si può ricavare dall'articolo 4, n. 12 GDPR, secondo cui per violazione dei dati personali deve intendersi una *"(...) 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*".
L'articolo 33 GDPR, rubricato "notifica di una violazione dei dati personali all'autorità di controllo", recita che "(*i)n caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente (...) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio dei diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dai motivi del ritardo*"
Qualora la violazione non avvenga presso il Titolare del trattamento, ma nei confronti del Responsabile, "*il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione*".
Bisogna innanzitutto precisare che il termine iniziale da cui far decorrere le 72 ore per procedere alla notifica deve necessariamente tenere conto del concetto di consapevolezza. A riguardo il Gruppo WP 29, nelle Linee Guida adottate il 3 ottobre 2017[29], ha affermato che *"(...) un Titolare debba essere considerato "consapevole" quando quel Titolare ha un ragionevole grado di certezza che si è verificato un incidente di sicurezza che ha portato a compromettere i dati personali. Ciò dipenderà dalle circostanze della specifica violazione. In alcuni casi, sarà relativamente chiaro fin dall'inizio che c'è stata una violazione, mentre in altri, potrebbe essere necessario del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto su un'azione tempestiva per indagare su un incidente per determinare se i dati personali sono stati effettivamente violati e, in caso affermativo, per intraprendere azioni correttive e notificare se necessario".*
Come specificato dal Gruppo WP29 la violazione dei dati personali può essere suddivisa in tre categorie:
– "*Confidentiality breach*": "violazione della riservatezza", in caso di divulgazione o accesso non autorizzato o accidentale a dati personali;
– "*Availability breach*": Violazione della disponibilità", in caso di perdita accidentale o non autorizzata di dati personali o di accesso o distruzione di dati personali;
– "*Integrity breach*": "violazione dell'integrità", in caso di modifica non autorizzata o accidentale di dati personali.
Ha precisato quindi che "*(...) una violazione può riguardare la riservatezza, la disponibilità e l'integrità dei dati personali allo stesso tempo, nonché qualsiasi combinazione di questi.*
Mentre determinare se vi sia stata una violazione della riservatezza o dell'integrità è relativamente chiaro, se vi è stata una violazione della disponibilità può essere meno ovvia. Una violazione sarà sempre considerata come una violazione della disponibilità in caso di perdita o distruzione permanente dei dati personali".
La notifica della violazione, ai sensi dell'articolo 33 GDPR, deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

29 Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 3 ottobre 2017

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

Qualora nel termine delle 72 ore successive al verificarsi della violazione, il Titolare non sia in possesso di tutte le informazioni, queste possono essere fornite successivamente ma senza ulteriore ingiustificato ritardo, fatto salvo l'obbligo di notifica nel termine di legge, motivando adeguatamente il motivo del ritardo.
Si richiama al riguardo il considerando 85 GDPR, il quale recita che *"una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo*".
Vi è in ogni caso l'obbligo di adeguata documentazione di tutte le violazioni dei dati personali, comprese le circostanze a esse relative, le conseguenze e i provvedimenti adottati per porvi rimedio, affinché l'Autorità di controllo possa procede alla verifica del rispetto della normativa vigente.
Al riguardo il GDPR non indica un termine minimo di conservazione della documentazione, lasciando così al Titolare del trattamento la libertà di determinare un appropriato termine di conservazione, nella misura in cui tale documentazione consenta all'Autorità di controllo di verificare il rispetto di tale articolo o, più in generale, del principio di responsabilizzazione.
L'articolo 34, rubricato "comunicazione di una violazione dei dati personali all'interessato", prevede l'obbligo della comunicazione della violazione "*quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche* (…)". In tal caso la violazione all'interessato deve essere comunicata senza ingiustificato ritardo.
La comunicazione deve essere fatta con un linguaggio semplice e chiaro, deve descrivere la natura della violazione dei dati personali e deve almeno:

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

Il considerando 86 specifica al riguardo che "*Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione*".
Ai sensi dell'articolo 34 par. 3, l'obbligo di comunicazione viene meno nei seguenti casi:

- *"il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;*
- *il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;*
- *detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si deve procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".*

Si precisa inoltre che "Il *WP29 raccomanda al Titolare di documentare anche il proprio ragionamento per le decisioni prese in risposta a una violazione. In particolare, se una violazione non viene notificata, deve essere documentata una giustificazione per tale decisione. Ciò dovrebbe includere le ragioni per le quali il Titolare del trattamento ritiene che la violazione non possa comportare un rischio per i diritti e le libertà delle persone. In alternativa, se il Titolare del trattamento ritiene che una delle condizioni di cui all'articolo 34, paragrafo 3, sia soddisfatta, dovrebbe essere in grado di fornire la prova adeguata che questo è il caso"*.
Qualora il Titolare del trattamento non abbia comunicato all'Interessato la violazione dei dati personali, l'Autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda, o può decidere che una delle condizioni sopra richiamate sia soddisfatta.
Stando a quanto sopra esposto, il GDPR prevede l'obbligo di notifica, con avvio della relativa procedura, nei confronti dell'Autorità qualora vi sia la probabilità che la violazione possa porre a rischio la libertà e i diritti degli individui, nei confronti degli interessati qualora vi sia la probabilità di un rischio elevato.
Ciò che rileva pertanto è la condotta in concreto tenuta dal Titolare del trattamento successivamente al verificarsi della violazione, anche a seguito della segnalazione da parte del Responsabile del trattamento, ovvero che si attivi applicando il protocollo implementato e formalizzato dall'azienda per il verificarsi di violazioni dei dati personali.
Proprio in questo senso il Gruppo WP 29 ha affermato *che "per agevolare la conformità con gli articoli 33 e 34, sarebbe vantaggioso sia per i titolari del trattamento che per i responsabili del trattamento disporre di una procedura di notifica documentata, che stabilisse la procedura da seguire una volta individuata una violazione, compreso come contenere, gestire e recuperare l'incidente, oltre a valutare i rischi e a notificare la violazione. A questo proposito, per dimostrare la conformità con GDPR potrebbe anche essere utile dimostrare che i dipendenti sono stati informati dell'esistenza di tali procedure e meccanismi e che sanno come reagire alle violazioni*".

2.2 La valutazione del rischio

L'obiettivo della valutazione del rischio (risk assessment) è quello di rilevare ed analizzare nel dettaglio l'assetto societario esistente al fine di effettuare una valutazione della conformità dello stesso rispetto al GDPR, così da effettuare un'analisi comparativa (la c.d. gap analysis) tra il modello organizzativo e di controllo esistente ("*as is*") e un modello astratto di riferimento valutato sulla base delle esigenze manifestate dalla normativa vigente ("*to be*").
Sulla base del risk assessment e del confronto operato con la gap analysis è stato possibile desumere le azioni di miglioramento del sistema interno esistente conformemente a quanto previsto dal GDPR.
La valutazione del rischio è stata effettuata esaminando tre questioni fondamentali: riservatezza, integrità e disponibilità dei dati trattati.
Al riguardo si riporta quanto prodotto da ENISA, L'Agenzia Europea per la sicurezza delle reti e delle informazioni, secondo la quale "*la riservatezza è definita come "la proprietà che le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati. In pratica, tutte le misure implementate per garantire la riservatezza sono progettate per impedire l'accesso alle informazioni da parte di individui, entità o processi non autorizzati, garantendo nel contempo che gli individui, le entità o i processi autorizzati possano accedervi. Nella maggior parte dei casi le informazioni sono classificate in base alla quantità e al tipo di danno che potrebbe essere fatto se dovesse cadere in mani non intenzionali. Misure più o meno rigorose possono quindi essere implementate in base a queste categorie.*

L'integrità è definita come la proprietà di "accuratezza e completezza". In questo senso, l'integrità implica il mantenimento della coerenza, dell'accuratezza e dell'affidabilità delle informazioni lungo l'intero ciclo di vita. I dati non devono essere modificati durante il trasporto e devono essere adottate misure per garantire che i dati non possano essere modificati da individui, entità o processi non autorizzati. Da un punto di vista pratico, ciò significa che i dati non possono essere modificati in modo non autorizzato o non individuato.
La disponibilità è definita come la proprietà di "informazioni accessibili e utilizzabili quando una parte autorizzata lo richiede". Ciò significa che i sistemi utilizzati per memorizzare ed elaborare le informazioni, così come i canali di comunicazione delle informazioni, funzionano tutti correttamente. In pratica, ciò è assicurato al meglio dalla manutenzione dell'hardware senza compromessi, eseguendo immediatamente riparazioni dell'hardware quando necessario e mantenendo un ambiente operativo del sistema operativo correttamente privo di conflitti software"[30].

Enisa afferma che la *"(v)alutazione del rischio (...) può essere intesa come la generazione di un'istantanea dei rischi attuali. Un rischio è spesso espresso in funzione della probabilità che un risultato avverso (minaccia) si verifichi, moltiplicato per la grandezza del risultato avverso (impatto) qualora si verifichi. La valutazione del rischio inizia con l'identificazione delle minacce, seguita dalla determinazione della pertinente probabilità e dell'impatto di ciascun rischio. Per valutare correttamente il rischio, bisogna prendere in considerazione allo stesso modo sia la probabilità che l'impatto.*
Sempre secondo Enisa, la valutazione del rischio deve essere effettuata con il seguente approccio:

1. Definizione dell'operazione di elaborazione e del suo contesto: in questa fase vengono esaminate le diverse fasi di elaborazione dei dati (dalla raccolta alla archiviazione fino alla cancellazione). Bisogna quindi interrogarsi su che tipo di operazioni vengono effettuate, che dati vengono trattati, qual è lo scopo del trattamento, quali sono i mezzi utilizzati per il trattamento dei dati personali, dove avviene il trattamento dei dati personali, quali sono le categorie di soggetti interessati, quali sono i destinatari dei dati;
2. Comprensione e valutazione dell'impatto: in questa fase viene valutato il potenziale impatto sui diritti e le libertà delle persone che un incidente di sicurezza (correlato al sistema di elaborazione dei dati) potrebbe avere. L'incidente di sicurezza deve essere associato a qualsiasi tipo di violazione della riservatezza, integrità o disponibilità dei dati. L'impatto è valutato in maniera qualitativa, avendo riguardo ai tipi di dati trattati, alla criticità dell'operazione di elaborazione, al volume di dati trattati, alle caratteristiche speciali del Titolare / Responsabile del trattamento, alle caratteristiche delle persone interessate e alla identificabilità delle stesse.

Pertanto, il metodo più diffuso per la misurazione del rischio inerente è dato dalla formula:

RISCHIO = IMPATTO X PROBABILITÀ

L'**impatto** indica gli effetti che la violazione delle regole in materia di privacy possono avere sui dati trattati.
L'impatto deve essere valutato in relazione alle libertà e ai diritti degli Interessati. Bisogna quindi prendere in considerazione gli effetti negativi che un individuo può subire, tra cui ad esempio il furto d'identità, la frode, la perdita finanziaria, danni fisici o psicologici, umiliazione, danni alla reputazione o addirittura minacce alla vita. In questa fase di analisi può non rilevare la scala di trattamento (numero di individui interessati), in quanto l'impatto potrebbe risultare elevato anche a fronte di un trattamento che riguardi una singola persona.
L'impatto deve essere valutato separatamente per la perdita di riservatezza, integrità e disponibilità, considerando tutti i possibili casi di divulgazione non autorizzata, alterazione o distruzione.
Si potranno ottenere così tre diversi livelli di impatto. Il risultato finale verrà valutato sulla base del risultato più alto ottenuto, considerato che si possono ottenere i seguenti risultati:

- Basso: Gli individui possono incontrare alcuni piccoli inconvenienti, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.);
- Medio: Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.);

30 Enisa, European Union Agency For Network and Information Security, "Guidelines for SMEs on the security of personal data processing", Dicembre 2016.

- Alto: Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento di liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.);
- Molto alto: gli individui possono avere conseguenze significative, o addirittura irreversibili, che non possono superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

3. Definizione di possibili minacce e valutazione della loro verosimiglianza (probabilità di occorrenza della minaccia). In questa fase è necessario comprendere le minacce e calcolare la probabilità di occorrenza avendo riguardo ai seguenti aspetti: risorse di rete e risorse tecniche (hardware e software), processi/procedure relativi alle operazioni di trattamento dei dati, persone coinvolte nelle operazioni di trattamento dei dati, settore aziendale e portata dell'elaborazione.

Per minaccia deve intendersi "(…) *qualsiasi circostanza o evento che possa influire negativamente sulla sicurezza dei dati personali. In questa fase, lo scopo dell'organizzazione è comprendere le minacce relative all'ambiente generale dell'elaborazione dei dati personali (esterni o interni) e valutare la loro probabilità (probabilità di occorrenza della minaccia)*". Anche in questa fase la valutazione deve essere effettuata avendo riguardo alla riservatezza, integrità e disponibilità dei dati personali. Enisa precisa inoltre che "*(...) il contesto dei dati personali (tipi di dati, soggetti dei dati, ecc.) non è considerato parte della probabilità di occorrenza della minaccia, in quanto è stato preso in considerazione durante la valutazione d'impatto*".

Come per la valutazione dell'impatto, la valutazione della **probabilità** può essere solo qualitativa, poiché correlata all'ambiente specifico di elaborazione dei dati personali.
All'esito di questa fase si potranno definire tre livelli di probabilità di occorrenza delle minacce:
- Basso: è improbabile che la minaccia si materializzi;
- Medio: è possibile che la minaccia si materializzi;
- Alto: la minaccia potrebbe realizzarsi.

La valutazione deve essere effettuata sulla base di questionari volti ad esaminare le aree sopra richiamate e che possono dare i seguenti risultati:

ASSESSMENT AREA	PROBABILITY	
	LEVEL	SCORE
NETWORK AND TECHNICAL RESOURCES	☐ Low	1
	☐ Medium	2
	☐ High	3
PROCESSES/PROCEDURES RELATED TO THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
PARTIES/PEOPLE INVOLVED IN THE PROCESSING OF PERSONAL DATA	☐ Low	1
	☐ Medium	2
	☐ High	3
BUSINESS SECTOR AND SCALE OF PROCESSING	☐ Low	1
	☐ Medium	2
	☐ High	3

Table 4: Assessing threat occurrence probability per area

La minaccia viene calcolata sommando i punteggi sopra ottenuti.

THREAT OCCURRENCE PROBABILITY SCALE	THREAT OCCURRENCE PROBABILITY LEVEL
4 - 5	Low
6 - 8	Medium
9 -12	High

Table 5: Evaluation of threat occurrence

2.3 Valutazione del rischio (combinando la probabilità di occorrenza della minaccia).

La valutazione finale del rischio può essere effettuata successivamente alla valutazione di impatto dell'operazione di trattamento e della relativa probabilità di occorrenza delle minacce.
Il livello di impatto è stato ponderato più della probabilità di occorrenza della minaccia e sono stati identificati solo due livelli di rischio basso e tre livelli di rischio medio. I livelli di impatto alto e molto alto sono stati tutti assegnati a livelli di rischio elevato e sono stati uniti.

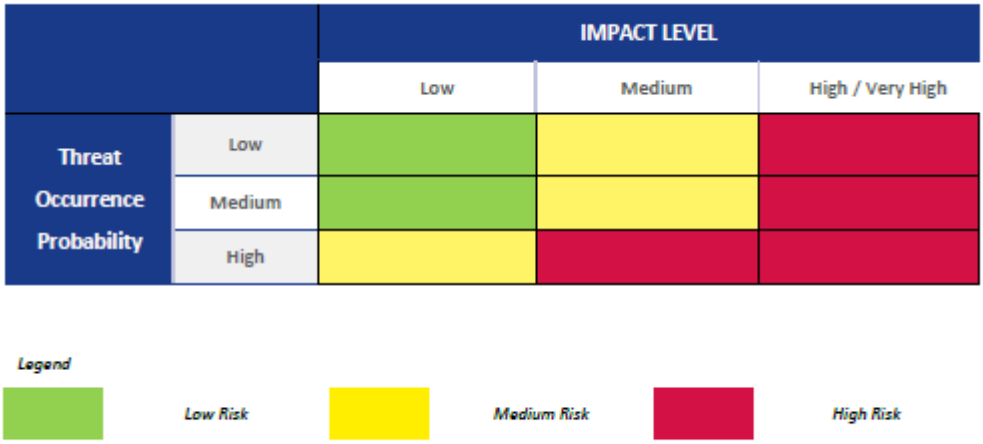

Table 6: Evaluation of risk

Come specificato da Enisa, "*indipendentemente dal risultato finale di questo esercizio, l'organizzazione dovrebbe sentirsi libera di adeguare il livello di rischio ottenuto, tenendo conto delle caratteristiche specifiche dell'operazione di trattamento dei dati (...) e fornendo un'adeguata giustificazione per tale adeguamento*".
Dalla valutazione del rischio discende l'applicazione delle misure tecniche, organizzative ed informatiche idonee a minimizzare e, qualora possibile, ad eliminare il rischio rilevato in fase di analisi.
Pertanto, un adeguato processo di gestione del rischio comprende ulteriori tre fasi:

- Il trattamento del rischio, ovvero la selezione e l'implementazione da parte dell'organizzazione di misure di sicurezza per il trattamento dei rischi. Tali misure possono avere differenti esiti: mitigazione, trasferimento, elusione o conservazione dei rischi.
- Accettazione del rischio qualora, anche a seguito del trattamento del rischio, rimangono dei rischi residui che devono essere accettati poiché in concreto non eliminabili. Si tratta di una decisione di gestione aziendale.
- Comunicazione del rischio, in quanto tutte le parti interessate devono essere informate sui rischi adottati e su quelli accettati.

In questo senso è importante evidenziare come le stesse misure tecniche ed organizzative adottate per la protezione dei dati personali devono essere commisurate al rischio rilevato a seguito della valutazione effettuata, ed in particolare avendo riguardo a natura, portata, contesto e finalità.
Enisa chiarisce al riguardo che "*(p)er raggiungere la scalabilità, si presume che tutte le misure descritte sotto il livello basso (verde) siano applicabili a tutti i livelli. Allo stesso modo, le misure presentate sotto il livello medio (giallo) sono applicabili anche ad alto livello di rischio. Le misure presentate sotto il livello alto (rosso) non sono applicabili a nessun altro livello di rischio.*
Va notato che la corrispondenza tra le misure e i livelli di rischio specifici non dovrebbe essere percepita come assoluta. A seconda del contesto del trattamento dei dati personali, l'organizzazione può considerare l'adozione di misure aggiuntive, anche se sono assegnate a un livello di rischio più elevato".
Le misure di sicurezza possono essere così riassunte:

1. Misure di sicurezza organizzative:
   - Politica della sicurezza e procedure per la protezione dei dati personali;
   - Chiara identificazione dei ruoli e delle responsabilità;
   - Politica di controllo di accesso ai sistemi utilizzati per il trattamento dei dati personali;
   - Gestione delle risorse (hardware, software e risorse di rete);
   - Gestione delle modifiche eseguite nel sistema IT;
   - Utilizzo di processori che garantiscano garanzie sufficienti per attuare misure tecniche e organizzative;
   - Data Breach e business continuity;

- Gestione delle risorse umane: riservatezza e formazione del personale.

2. Misure tecniche di sicurezza:
Le misure di sicurezza devono tenere conto dei seguenti aspetti:

- Controllo degli accessi e autenticazione, per la protezione contro l'accesso non autorizzato al sistema informatico utilizzato per il trattamento dei dati personali;
- Registrazione e monitoraggio, mediante l'utilizzo di file di registro (log files) per l'identificazione e il tracciamento delle azioni effettuate dagli utenti, al fine di individuare possibili tentativi interni o esterni di violazione del sistema;
- Sicurezza dei dati a riposo, ovvero avendo riguardo alle modalità di trattamento dei dati in banche dati o altri sistemi pertinenti (compreso il salvataggio in cloud) e alle modalità di trattamento dei dati da parte di dipendenti con l'uso di postazioni specifiche o altri dispositivi. Si deve anche avere riguardo alla sicurezza del server/database e alla sicurezza delle workstation degli utenti o di altri dispositivi;
- Sicurezza della workstation degli utenti o di altri dispositivi;
- Sicurezza della rete avendo riguardo a connessioni esterne e alle interconnessioni con altri sistemi (interni o esterni dell'organizzazione);
- Back-up, in quanto è un mezzo essenziale per recuperare dalla perdita o distruzione dei dati;
- Dispositivi mobili / portatili;
- Sicurezza del ciclo di vita delle applicazioni;
- Cancellazione / eliminazione dei dati in modo irreversibile affinché non possano essere recuperati;
- Sicurezza fisica, al fine di limitare gli accessi fisici al sistema informativo.

La valutazione del rischio è stata effettuata con l'ausilio di:

- documenti sviluppati da ENISA (Guidelines for SME on the security of personal data processing e Handbook on Security of Personal Data Processing);
- documenti sviluppati da ENISA per la valutazione del rischio (2007-2008);
- software rilasciato dal CNIL per la valutazione di impatto.

3 Approccio metodologico

L'adeguamento societario al nuovo GDPR è avvenuto in maniera progressiva, secondo un piano di lavoro che può essere così riassunto:

DESCRIZIONE	ATTIVITÁ SVOLTA
Acquisizione ed esame della documentazione societaria	- invio check list documenti necessari per l'analisi della struttura organizzativa e dei dati trattati - utilizzo di una check list per l'analisi preliminare - valutazione ed analisi dei documenti acquisiti e dei risultati della check list
Organizzazione e governance	- esame dei processi e delle politiche aziendali, degli aspetti organizzativi e legali, dei sistemi informativi adottati (IT governance) e della corretta individuazione dei soggetti direttamente coinvolti.
Intervista ai key officer	- svolgimento di interviste singole o di gruppo sulla base di specifiche check list
Adeguamento delle informative e gestione del consenso	- Adeguamento rispetto ai trattamenti effettuati e dei consensi prestati circa il nuovo obbligo di informativa da fornire ai soggetti Interessati sia off-line che on-line (sito/ e-commerce)

Responsabili esterni del trattamento	- Predisposizione del contratto con i Responsabili esterni del trattamento
Valutazione del rischio	- Valutazione del rischio ai fini della determinazione delle misure tecniche e organizzative adeguate da implementare
Data Protection Impact Assessment (qualora necessaria)	- Redazione della Data Protection Impact Assessment sulla base anche dei documenti sviluppato da ENISA (Guidelines for SME on the security of personal data processing e Handbook on Security of Personal Data Processing) con l'ausilio del software rilasciato dal CNIL qualora necessaria per la tipologia di trattamenti
Data Protection Officer	- Preliminare valutazione sulla necessità di nominare il DPO
Registro del Titolare del trattamento	- Creazione e compilazione del Registro del Titolare del trattamento
Registri Protezione Dati	- Creazione e consegna dei Registri Protezione Dati
Modello organizzativo Privacy	- definizione di un modello organizzativo della privacy con relativi protocolli - redazione delle policy necessarie sulla base della valutazione del rischio
Formazione	- formazione in aula con i soggetti direttamente coinvolti con un piano formativo da individuare sulla base dei risultati emersi in sede di analisi e delle procedure implementate

4 Sistema sanzionatorio

L'articolo 83 GDPR disciplina l'applicazione delle sanzioni amministrative pecuniarie che possono essere inflitte sia nei confronti di persone fisiche che nei confronti di persone giuridiche pubbliche o private, ovvero nei confronti del Titolare del trattamento e del Responsabile del trattamento, dei Rappresentanti ecc.
Le sanzioni amministrative pecuniarie possono arrivare fino a:

- 10 milioni di euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei seguenti casi:
  - Violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società di informazione, di cui all'articolo 8 GDPR;
  - Trattamento illecito di dati personali dell'Interessato che non richiede l'identificazione dell'Interessato, di cui all'articolo 11 GDPR;
  - Violazione degli obblighi di cui agli articoli da 25 a 39, ovvero:
    - Principi e misure di data protection by design e by default;
    - Accordo interno per determinare le responsabilità tra contitolari del trattamento;
    - Nomina del Rappresentante di titolari del trattamento o dei Responsabili del trattamento non stabiliti nel territorio dell'Unione e suoi compiti;
    - Mansioni e responsabilità del Responsabile del trattamento;
    - Trattamento sotto l'autorità del Titolare o del Responsabile del trattamento;
    - Tenuta dei registri dell'attività del trattamento;
    - Cooperazione del Titolare o del Responsabile con l'Autorità di controllo;
    - Adozione di misure di sicurezza adeguate;

- Notifica di una violazione dei dati personali all'Autorità di controllo;
- Comunicazione di una violazione dei dati personali all'interessato;
- Valutazione d'impatto sulla protezione dei dati trattati e consultazione preventiva dell'Autorità di controllo se la valutazione di impatto evidenzia un rischio elevato;
- Designazione del DPO;
- Obblighi del Titolare e del Responsabile nei confronti del DPO;
- Esecuzione dei propri compiti da parte del DPO.

Le medesime sanzioni sono applicate, ai sensi dell'articolo 166 comma 1, D.lgs 196/03, così come modificato dal D.lgs. 10 agosto 2018, n. 101[31], nei seguenti casi:

Articolo 2-quinquies, comma 2	Violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
Articolo 2 - quinquiesdecies	Violazione delle disposizioni per trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico
Articolo 92 comma 1	Violazione delle disposizioni in materia di tenuta delle cartelle cliniche da parte di strutture, pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie
Articolo 93 comma 1	Certificato di assistenza al parto
Articolo 123 comma 4	Violazione delle disposizioni in materia di informativa da rendere nei servizi di comunicazione elettronica
Articolo 128	Violazione delle disposizioni relative al trasferimento automatico della chiamata nei servizi di comunicazione elettronica
Articolo 129 comma 2	Violazione delle disposizioni relative agli elenchi dei contraenti nei servizi di comunicazione elettronica
Articolo 132 ter	Violazione delle disposizioni in materia di sicurezza del trattamento nei servizi di comunicazione elettronica
Articolo 110 comma 1 primo periodo	Omessa valutazione di impatto in materia di ricerca medica, biomedica ed epidemologica
Articolo 110 comma 1 terzo periodo	Omessa consultazione preventiva del Garante del programma di ricerca medica, biomedica ed epidemologica

- 20 milioni di euro, o per le imprese, fino a 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nei seguenti casi:
  - Violazione dei principi generali applicabili al trattamento, di cui all'art. 5 GDPR;
  - Violazione delle condizioni di liceità per il trattamento di cui all'art. 6 GDPR;
  - Violazione delle condizioni per il consenso e diritto di revoca di cui all'art. 7 GDPR;
  - Violazione delle disposizioni relative al trattamento di categorie particolari di dati (sensibili giudiziari) di cui all'art. 9 GDPR;
  - Mancato rispetto dell'esercizio dei diritti degli interessati di cui agli artt. da 12 a 21 GDPR;
  - Violazione delle norme relative al processo automatizzato, compresa la profilazione, di cui all'art. 22 GDPR;

31 Decreto Legislativo 10 agosto 2018, n. 101: Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati).

- Violazione delle norme concernenti il trasferimento dei dati a un destinatario in un paese terzo o a un'organizzazione internazionale di cui agli artt. Da 44 a 49 GDPR;
- Violazione di qualsiasi altra norma/obbligo adottata a livello nazionale, in tema di: rapporti di lavoro, archivi storici, ricerca scientifica o storica o statistica, titolari soggetti a segreto professionale, chiese e associazioni religiose e di qualsiasi inosservanza di ordini, limitazioni provvisorie o definitive adottate dalle singole Autorità competenti in funzione correttiva ex art. 58.2 GDPR o per negato accesso durante l'esercizio dei poteri di indagine ex art. 58.1 GDPR.

Le medesime sanzioni sono applicate, ai sensi dell'articolo 166 comma 2, D.lgs. 196/03, così come modificato dal D.lgs. 10 agosto 2018, n. 101, nei seguenti casi:

Articolo 2-ter	Violazione dei principi applicabili (base giuridica) per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri
Articolo 2-quinquies, comma 1	Violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione
Articolo 2-sexies	Violazione delle disposizioni concernenti il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante
Articolo 2-septies, comma 7	Violazione delle misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute, con riguardo alle procedure di accesso fisico e logico ai dati
Articolo 2-octies	Violazione dei principi relativi al trattamento dei dati relativi a condanne penali e reati
Articolo 2-terdecies, commi 1,2,3 e 4	Violazione dei diritti riguardanti le persone decedute
Articolo 52, commi 4 e 5	Violazione delle disposizioni concernenti i dati identificativi degli Interessati, avendo riguardo ai trattamento in ambito giudiziario e nello specifico all'Informatica giuridica
Articolo 75	Violazione delle specifiche condizioni di trattamento in ambito sanitario
Articolo 78	Violazione delle disposizioni riguardanti le informazioni del medico di medicina generale o del pediatra
Articolo 79	Violazione delle disposizioni riguardanti le informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie
Articolo 80	Violazione delle disposizioni riguardanti le informazioni da parte di altri soggetti
Articolo 82	Violazione delle disposizioni concernenti emergenze e tutele della salute e dell'incolumità fisica
Articolo 92, comma 2	Violazione delle disposizioni concernenti la corretta tenuta delle cartelle cliniche
Articolo 93 commi 2 e 3	Violazione delle disposizioni concernenti il certificato di assistenza al parto
Articolo 96	Violazione delle disposizioni concernenti il trattamento di dati relativi a studenti nell'istruzione

Articolo 99	Violazione delle disposizioni concernenti la durata del trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici
Articolo 100, commi 1, 2 e 4	Violazione delle disposizioni concernenti i dati relativi ad attività di studio e di ricerca
Articolo 101	Violazione delle disposizioni concernenti le modalità di trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica
Articolo 105 commi 1, 2 e 4	Violazione delle disposizioni concernenti le modalità di trattamento dei dati a fini statistici o di ricerca scientifica
Articolo 110 bis, commi 2 e 3	Violazione delle disposizioni concernenti il trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici
Articolo 111	Violazione delle regole deontologiche per i trattamenti nell'ambito di rapporto di lavoro
Articolo 111-bis	Violazione delle disposizioni concernenti le informazioni da fornire in caso di ricezione di curriculum nell'ambito del rapporto di lavoro
Articolo 116, comma 1	Violazione delle disposizioni concernenti la conoscibilità di dati su mandato dell'Interessato relativamente agli istituti di patronato e di assistenza sociale
Articolo 120, comma 2	Violazione delle disposizioni in ambito assicurativo (sinistri)
Articolo 122	Violazione delle disposizioni concernenti le informazioni raccolte nei riguardi del contraente o dell'utente in ambito di comunicazioni elettroniche
Articolo 123, commi 1, 2, 3 e 5	Violazione delle disposizioni concernenti i dati relativi al traffico in ambito di comunicazioni elettoniche
Articolo 124	Violazione delle disposizioni concernenti la fattura dettagliata in ambito di comunicazioni elettroniche
Articolo 125	Violazione delle disposizioni concernenti l'identificazione elettronica in ambito di comunicazioni elettroniche
Articolo 126	Violazione delle disposizioni concernenti i dati relativi all'ubicazione
Articolo 130, commi da 1 a 5	Violazione delle disposizioni concernenti le comunicazioni indesiderate
Articolo 131	Violazione delle disposizioni relative alle informazioni da fornire a contraenti e utenti nell'ambito delle comunicazioni elettroniche
Articolo 132	Violazione delle disposizioni relative alla conservazione di dati di traffico delle comunicazioni elettroniche per altre finalità
Articolo 132-bis, comma 2	Violazione delle procedure istituite dai fornitori in materia di comunicazioni elettroniche
Articolo 132-quater	Violazione delle disposizioni relative alle informazioni sui rischi da parte dei fornitori dei servizi di comunicazione elettronica
Articolo 157	Mancato conferimento di informazioni o omessa esibizione di documenti su richiesta dell'Autorità di Controllo
Articolo 2-quater	Violazione di regole deontologiche

Articolo 2-septies	violazione di misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute

Le sanzioni imposte dal nuovo GDPR sono volte ad armonizzare il sistema sanzionatorio in tutto il territorio dell'Unione Europea, lasciando alle singole Autorità competenti e ai singoli Stati membri il compito di determinare le stesse. Le sanzioni di cui all'articolo 83 GDPR devono essere infatti adottate in aggiunta alle misure correttive di cui all'articolo 58.2 GDPR[32] . Tale principio viene affermato anche dal Considerando 148, il quale recita che, la singola Autorità competente, oltre a dover prevedere delle sanzioni pecuniarie amministrative in aggiunta o in sostituzione di quelle imposte dall'Autorità di controllo nel GDPR, "*in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una pena pecuniaria*". Il legislatore europeo ha deciso pertanto di cercare di uniformare il diritto dell'Unione, anche sotto un punto di vista sanzionatorio, ma lasciando comunque una libertà "vincolata" alle singole Autorità, e per l'effetto ai singoli Stati. Con il D.lgs. n. 101 del 10 agosto 2018 si è cercato quindi di reperire dare attuazione a quanto deposito a livello europeo, tenendo comunque presente che le sanzioni devono essere effettive, proporzionate e dissuasive, e che devono tenere debito conto 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;
- 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, 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.

Se, in relazione allo stesso trattamento o a trattamenti collegati, un Titolare del trattamento o un Responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo

32 Art. 58.2 GDPR: " (…) *Ogni autorità di controllo ha tutti i poteri correttivi seguenti: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento; d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19; h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti; i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale".*

totale della sanzione amministrativa pecuniaria non può superare l'importo specificato per la violazione più grave.
L'Autorità di Controllo (Garante) è l'organo competente ad adottare sia i provvedimenti di cui all'articolo 58 par. 2 GDPR che ad irrogare le sanzioni sopra esposte.
Contro l'irrogazione delle suddette sanzioni sarà possibile proporre ricorso giurisdizionale secondo il diritto nazionale.
Ai sensi dell'articolo 84 GDPR, è possibile per i singoli Stati membri stabilire ulteriori norme e sanzioni in aggiunta a quelle di cui sopra. La lettura in combinato disposto di questo articolo con il Considerando 149 GDPR, ha lasciato aperta la possibilità per i singoli Stati membri di prevedere sanzioni penali per la violazione della normativa europea, nei confronti delle persone fisiche che hanno commesso o hanno concorso a commettere il fatto, in ossequio del principio Societas delinquere non potest, secondo cui la responsabilità penale è personale e non può essere applicata nei confronti delle persone giuridiche, permanendo così in capo all'ente la sola responsabilità amministrativa (pena pecuniaria) e l'obbligo di adempiere alle misure correttive.
In questo senso, il D.lgs. 101/2018 ha delineato il seguente quadro sanzionatorio:

ARTICOLO	TESTO
Articolo 167 D.lgs. 196/03: *Trattamento illecito di dati*	*1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.*
	2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, e' punito con la reclusione da uno a tre anni.
	3. Salvo che il fatto costituisca piu' grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sè o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
	(....)
	6.Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita
Articolo 167-bis D.lgs. 196/03: *Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*	*1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.*
	2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

	Per i reati di cui ai commi 1 e 2, si applicano i commi (....) 6 dell'articolo 167
Articolo 167-ter D.lgs. 196/03: *Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*	*1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.*
	2. Per il reato di cui al comma 1 si applicano i commi (....) 6 dell'articolo 167
Articolo 168 D.lgs. 196/03: *Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*	*1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.*
	2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.
Articolo 170 D.lgs. 196/03: *Inosservanza di provvedimenti del Garante*	*1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonchè i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 e' punito con la reclusione da tre mesi a due anni.*
Articolo 171 D.lgs. 196/03: Violazione delle dispo*sizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori*	*La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, e' punita con le sanzioni di cui all'articolo 38 della medesima legge.*

	Articolo 4 Legge 20 maggio 1970, n. 300: *Impianti audiovisivi* *1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.* *2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.* *3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.* Articolo 8 Legge 20 maggio 1970, n. 300*: Divieto di indagini sulle opinioni* *1.È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.* Articolo 38 Legge 20 maggio 1970, n. 300*: Disposizioni penali* *1. Le violazioni degli articoli 2, 5, 6 e 15, primo comma lettera a), sono punite, salvo che il fatto non costituisca più grave reato, con l'ammenda da lire 300.000 a lire 3.000.000 o con l'arresto da 15 giorni ad un anno.* *2. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente.* *3. Quando per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.* *4. Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale.*
Articolo 172 D.lgs. 196/03: *Pene accessorie*	*1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza ai sensi dell'articolo 36, secondo e terzo comma, del codice penale.*

Resta ferma inoltre la possibilità per il singolo Interessato che ha subito una violazione nel trattamento dei propri dati personali di agire in giudizio per ottenere il risarcimento del danno.
Al riguardo si specifica che l'articolo 82 GDPR, ponendo l'attenzione ai diritti dell'Interessato al trattamento, prevede la possibilità per colui che subisce un danno materiale o immateriale di ottenere il risarcimento del danno, indistintamente dal Titolare del trattamento o dal Responsabile del trattamento, configurando così una responsabilità di tipo solidale in capo agli stessi al fine di garantire l'effettivo risarcimento dell'interessato.

Titolare e Responsabile sono quindi responsabili ognuno per i danni causati dall'inottemperanza agli obblighi del GDPR, con contestuale esonero esclusivamente previa dimostrazione che l'evento dannoso non sia in alcun modo imputabile alla condotta tenuta.
Avendo infatti il legislatore europeo previsto una responsabilità di tipo solidale in capo al Titolare e al Responsabile del trattamento, il terzo Interessato può agire indistintamente nei confronti del Titolare o del Responsabile, rimanendo nei confronti del soggetto chiamato a risarcire il danno esclusivamente la possibilità di agire di rivalsa nei confronti dell'altro soggetto. Proprio per queste ragioni si è insistito sulla necessità di stipulare appositi contratti tra il Titolare del trattamento e i propri Responsabili esterni, al fine di stabilire le modalità di gestione dei dati stessi. L'adempimento di tutti i doveri è condizione necessaria per evitare che vengano a crearsi ipotesi di responsabilità nei confronti dell'interessato del trattamento.

5 Parte Speciale

5.1 Dati identificativi del Titolare e sedi

Denominazione	ORDINE PROVINCIALE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DI MODENA
Sede legale ed operativa	MODENA (MO), PIAZZALE BOSCHETTI N. 8 – CAP 41121 –
Codice Fiscale/P.IVA	80095150365 --
Durata	--------N.A.----------

5.2 Forma giuridica

Il Titolare opera quale ente pubblico non economico.

6 Descrizione dell'attività

Espletamento di tutte le attività previste dalla normativa vigente quale ente pubblico non economico.

7 La valutazione del rischio

7.1 Risultati della valutazione del rischio

La valutazione del rischio del Titolare, effettuata con la modalità indicata ai punti 2.2 e 2.3, ha evidenziato un rischio "MEDIO".
La valutazione è reperibile all'interno del Registro del Titolare del trattamento.

Il Titolare ha proceduto alla redazione della Data Protection Impact Assessment per i seguenti trattamenti:

- Trattamento dei dati personali e particolari dei Medici Iscritti.

Non si è proceduto, in questa prima fase, alla redazione della Data Protection Impact Assessment per gli ulteriori trattamenti effettuati dal Titolare nello svolgimento della propria attività in quanto non sussistono gli elementi e le condizioni di cui al punto 2 lett. d) del presente Modello, come evidenziato nella valutazione del rischio preliminare reperibile all'interno del Registro del Titolare del trattamento.
Il Titolare ha inoltre attuato misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli Interessati.
In questo senso, il Titolare si impegna a monitorare e se del caso aggiornare i trattamenti effettuati nello svolgimento delle proprie attività, al fine di valutare continuamente i rischi creati nello svolgimento delle stesse e procedere, se del caso, all'aggiornamento della Data Protection Impact Assessment o alla redazione della stessa per gli ulteriori trattamenti effettuati.

All’esito della valutazione del Rischio effettuata e della mappatura dei trattamenti effettuati, il Titolare ha proceduto con la nomina del Data Protection Officer (DPO).

8 Misure di sicurezza

8.1 Misure di sicurezza tecniche e organizzative

All’esito della valutazione del rischio, il Titolare implementa le misure tecniche e organizzative adeguate al rischio emerso.
Le misure di sicurezza sono reperibili all’interno del Registro del Titolare del trattamento. È stato previsto di indicare lo status della misura (attivo, in approfondimento, in attesa, implementazione futura, non implementabile, non applicabile), il soggetto al quale è in carico l’implementazione ed eventuali note.

9 Il Registro del Titolare del trattamento

9.1 Contenuto

Il Registro del Titolare del trattamento, oltre a quanto indicato nei paragrafi precedenti, contiene la descrizione di tutti i trattamenti svolti dal Titolare, l’elenco dei Responsabili del trattamento, i Protocolli eventualmente adottati e le Informative per la protezione dei dati.
Nella sezione “Trattamenti”, sono indicate delle eventuali misure di sicurezza specifiche per quel singolo trattamento. Ciò significa che, se tale sezione è compilata, le misure ivi indicate si applicano in deroga alle misure tecniche e organizzative previste nella sezione “Misure di sicurezza”; in caso contrario a tutti i trattamenti si applicano le misure tecniche e organizzative indicate nella sezione “Misure di sicurezza”.
Nella sezione “Responsabili del trattamento”, vengono indicati i responsabili che trattano i dati del Titolare, il contratto sul quale si basano i trattamenti e le misure previste.
Infine, nella sezione “Protocolli/Informative per la protezione dei dati”, è previsto l’inserimento di tutti i protocolli eventualmente adottati, delle policy con indicazione dei soggetti destinatari, la revisione, la modalità di comunicazione, la data di creazione, di aggiornamento, con indicazione del successivo aggiornamento.

10 Registri Protezione Dati

10.1 Contenuto

I “Registri Protezione Dati”, è un documento utile al Titolare per mappare la propria rete informatica e i soggetti che accedono ai dati. In particolare, la sezione “Registro dei dispositivi”, permette di inserire la mappatura dei dispositivi e l’indicazione del soggetto che ha in uso e/o accede ai medesimi; la sezione “Incaricati”, consente di inserire il ruolo dell’incaricato all’interno della struttura, indicando l’account di posta in uso, l’eventuale accesso al gestionale etc.
La sezione denominata “Registro degli Eventi”, consente di indicare le operazioni svolte dall’Amministratore di Sistema, manualmente, nell’ambito delle funzioni a lui attribuite dalla Carta IT.
Infine, è stato inserito il “Registro delle Violazioni”, per la cui compilazione si rimanda al Protocollo sul Data Breach.

11 Allegati

Al presente Modello vengono allegati:

a) RISK ASSESSMENT e GAP ANALYSIS
b) Registro del Titolare del trattamento
c) Registri Protezione Dati
d) Protocollo Data Breach
e) Carta IT
f) Piano di Business Continuity
g) Politica di Sicurezza delle Informazioni
h) Analisi Tecnico-Informatica
i) Organigramma