ASP
centro servizi alla persona

GDPR IN BREVE

Oggetto del Regolamento

Il GDPR stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali , nonché norme relative alla libera circolazione di tali dati . Si applica a tutti i tipi di trattamento, non automatizzato, interamente o parzialmente automatizzato.

Alcune definizioni

«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.

«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.

«Categorie particolari di dati» : dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici[1] , dati biometrici[2] intesi a identificare in modo univoco una persona fisica, dati relativi alla salute[3] o alla vita sessuale o all'orientamento sessuale della persona.

«***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.

«***Profilazione***» : qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati, 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

[1] Art. 4 - «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.

[2] Art. 4 - «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.

[3] Art. 4 - «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.

preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

«Pseudonimizzazione» : il trattamento dei dati personali in modo tale che tali dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni 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.

I diversi attori

«***Interessato***» : la persona fisica a cui si riferiscono i dati trattati, ottenuti direttamente dall'interessato, o tramite altra fonte. Presso ASP si possono individuare diverse categorie di interessati, primi fra tutti gli utenti dei servizi e loro familiari, ma anche il personale, i collaboratori, i fornitori ecc.

«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. ASP è titolare dei dati di cui determina le finalità e i mezzi del trattamento.

«Contitolari del trattamento» : due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento , determinando altresì, in modo trasparente, mediante un accordo interno , le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato. Occorre valutare caso per caso se si è in presenza di contitolarità. Il rapporto tra le parti è paritario se viene assunta una codecisione sulle finalità e sui mezzi di un determinato trattamento da parte dei soggetti che esercitano l'effettivo potere decisorio in relazione al trattamento dei dati personali.

«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. In tal caso il titolare del trattamento 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 Regolamento e garantisca la tutela dei diritti dell'interessato. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico . Questa fattispecie si può configurare, a titolo di esempio, nel caso in cui ASP stipuli un contratto, a seguito di gara pubblica, con una impresa esterna per la gestione di Centri socio riabilitativo per persone diversamente abili utenti dei servizi.

«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. ASP, nell'attuazione dei propri compiti istituzionali, deve trasmettere dati personali ad altri enti, ad esempio INPS, strutture sanitarie, ecc..

«Soggetti autorizzati» : i soggetti che hanno accesso ai dati personali, in quanto effettuano materialmente le operazioni di trattamento sui dati stessi. Possono operare sotto la diretta autorità del titolare ma anche del responsabile, se nominato. Tali soggetti devono essere istruiti. E' pertanto organizzata adeguata formazione e saranno predisposte le necessarie istruzioni operative, comprensive degli obblighi inerenti le misure di sicurezza. I soggetti autorizzati dovranno attenersi alle istruzioni ricevute.

«Responsabile della protezione dei dati» : tale figura svolge i seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

ASP ha individuato come responsabile della protezione dei dati la Società Lepida, con sede a Bologna in via della Liberazione 15 .

I principi

«Liceità, correttezza e trasparenza» : i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

«Limitazione della finalità» : i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità ; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali.

«Minimizzazione dei dati» : i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

«Esattezza»: i dati devono essere esatti e, se necessario, aggiornati ; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

«Limitazione della conservazione»: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1[4] , fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.

[4] Art. 89 paragrafo 1 - Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere

«Integrità e riservatezza» : i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali , compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

«Responsabilizzazione» : il titolare del trattamento deve essere in grado di comprovare il rispetto dei suddetti principi.

I fondamenti di liceità del trattamento

Il trattamento, per essere «lecito» si deve fondare su una delle seguenti «basi giuridiche» :

- **«consenso** » : l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

- «**adempimento di obblighi contrattuali** » : il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

- «obblighi legali » : il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

- «**interessi vitali dell'interessato o di terzi** »[5] : il trattamento è necessario per la salvaguardia degli 5 interessi vitali dell'interessato o di un'altra persona fisica;

- **«interesse pubblico o esercizio di pubblici poteri»** : il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

- «**interesse legittimo del titolare o di terzi cui i dati vengono comunicati**»[6] : il trattamento è 6 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. Ciò non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Le categorie particolari di dati

Il Regolamento vieta di trattare le categorie particolari di dati, ma stabilisce altresì che tale divieto non si applica se si verifica uno dei seguenti casi:

---

conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

[5] Interesse vitale di un terzo: si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione

[6] Interesse legittimo prevalente di un titolare o di un terzo: il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato è compito del titolare. L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità. Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti

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;

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 riguarda dati personali resi manifestamente pubblici dall'interessato;

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

f. 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;

g. 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[7] ;

h. 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;

i. 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[8] , sulla base del diritto dell'Unione o nazionale, che

[7] Art. 9 paragrafo 3 - I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

[8] Art. 89 paragrafo 1 - Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

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.

Le informazioni all'interessato

ASP, in qualità di titolare, deve fornire informazioni all'interessato in base a quanto stabilito negli articoli 13 e 14.

Se i dati sono raccolti presso l'interessato (art. 13), l'informativa deve essere fornita prima di effettuare la raccolta dei dati.

Se i dati non sono raccolti direttamente presso l'interessato (art. 14), l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato). L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online.

Spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.

Ogni volta che le finalità cambiano, il Regolamento impone di informare l'interessato, prima di procedere al trattamento ulteriore.

Il consenso

Qualora il trattamento sia basato sul « consenso dell'interessato » il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Non è ammesso il consenso tacito o presunto (non vanno bene caselle pre-spuntate su un modulo). L'interessato ha il diritto di revocare il consenso in qualsiasi momento.

Il consenso dei minori è valido a partire dai 16 anni (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Alla luce di quanto sopra e allo scopo di garantire un'efficace protezione dei dati personali, ASP, in qualità di titolare del trattamento, deve assicurare il rispetto delle disposizioni del Regolamento.

Più in particolare deve:

1) tenere un « ***registro delle attività di trattamento*** » (art. 30): si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti posti in essere all'interno di ASP, indispensabile per la valutazione e l'analisi dei rischi. Tale registro deve essere esibito al Garante per la protezione dei dati personali, su sua richiesta;

2) acquisire il « ***consenso*** » , ove necessario (artt. 7, 8 e 9)

3) fornire « i***nformazioni*** » all'interessato (artt. 13 e 14);

4) garantire l'esercizio dei diritti agli interessati: diritto di accesso (art. 15); diritto di rettifica (art. 16); diritto alla cancellazione o «diritto all'oblio» (art. 17); diritto di limitazione di trattamento (art. 18); diritto di opposizione (art. 21). Nel caso di esercizio di tali diritti, il termine per rispondere all'interessato è un mese,

estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego;

5) **« *istruire »*** i soggetti che hanno accesso a dati personali (art. 29);

6) nominare i « ***responsabili del trattamento*** » (art. 28);

7) proteggere i dati fin dalla progettazione (art. 25): 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;

8) proteggere i dati per impostazione predefinita (art. 25): 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;

9) mettere in atto, riesaminare e aggiornare, « ***misure tecniche e organizzative adeguate*** » per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento, 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. Se ciò è proporzionato rispetto alle attività di trattamento, tali misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento (art. 32);

10) «***notificare*** » al Garante per la protezione dei dati personali, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, la violazione dei dati personali, 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, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (art. 33);

11) « ***comunicare la violazione dei dati personali all'interessato*** » , senza ingiustificato ritardo, quando è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 34);

12) effettuare una «***valutazione d'impatto del trattamento dei dati personali*** » , prima di procedere al trattamento stesso, consultandosi con il Responsabile della protezione dei dati. Tale valutazione deve essere svolta nel caso in cui 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 medesimo, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi;

13) effettuare una « ***consultazione preventiva del Garante per la protezione dei dati personali*** » , prima di procedere al trattamento. Tale consultazione è prevista qualora la suddetta valutazione d'impatto indichi

che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio (art. 35);

14) ***«designare un responsabile della protezione dei dati*** » (art. 37) con le caratteristiche e le funzioni previste negli articoli 38 e 39. Tale figura ha il compito di fornire consulenza ad ASP come Titolare del trattamento dei dati personali, ma al tempo stesso di sorvegliare sull'osservanza del GDPR.