Vademecum sul Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation). Rev. 1.0

Indice

Premessa

A partire dal 25 maggio 2018 è direttamente applicabile in tutti gli Stati membri il Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) – relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali. (di seguito, Regolamento)

Il Regolamento nasce dalla necessità di predisporre **maggiori tutele a favore dei diritti e delle libertà dei cittadini** oltre alla volontà – da parte del Legislatore comunitario - di assicurare: certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Ue verso altre parti del mondo.

Cosa cambia con il Regolamento generale sulla protezione dei dati:

- ✓ Viene ridisegnato l'organigramma aziendale privacy
- ✓ Si introducono regole più chiare su informativa e consenso;
- ✓ Vengono definiti i limiti al trattamento automatizzato dei dati personali;
- ✓ Poste le basi per l'esercizio di nuovi diritti;
- ✓ Stabiliti criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue;
- ✓ Fissate norme rigorose per i casi di violazione dei dati (data breach).
- ✓ Le norme si applicano anche alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti all'interno del mercato Ue. Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le nuove regole. Imprese ed enti avranno più responsabilità e in caso di inosservanza delle regole rischiano pesanti sanzioni.
- ✓

I dati personali presi in esame e oggetto di tutela dal Regolamento sono solo quelli relativi a persone fisiche.

Il Regolamento, quindi, non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

1. I principi in materia di trattamento dei dati personali

Il **principio di trasparenza** previsto dal Regolamento, è, forse, il principio che maggiormente è divenuto oggetto dell'intervento modificativo operato dal Legislatore europeo, volto a rafforzarne la portata.

Il nucleo è il seguente: le informazioni che il Titolare del trattamento deve fornire all'interessato con riferimento alle modalità di trattamento dei suoi dati, devono sempre essere rese in **forma concisa, trasparente, intelligibile e facilmente accessibile,** con un linguaggio semplice e chiaro.

Nel caso, poi, l'interessato effettui una richiesta specifica chiedendo l'accesso ai dati, la rettifica, la cancellazione, una limitazione del trattamento, o la portabilità degli stessi, le informazioni oggetto della richiesta devono essere rese senza ritardo e, al più tardi, entro un mese dal ricevimento della richiesta (se ci sono comprovate difficoltà nel reperimento dei dati il termine può essere prorogato di altri 30 g.)

Principio di necessità. Ci si riferisce ai trattamenti dei dati svolti con sistemi automatizzati che devono essere configurati in modo da minimizzare il ricorso a dati personali e identificativi, sostituendone il trattamento con l'uso di dati anonimi e prevedendo l'identificazione dell'interessato solo in caso di necessità. Dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano (ad es. mediante dichiarazione scritta od orale). Non dovrebbero configurare consenso il silenzio, la inattività o la preselezione di caselle.

Principio di liceità e correttezza. Si richiede che i dati personali siano trattati in modo lecito e secondo correttezza, siano raccolti per finalità esplicite, legittime e determinate e che il trattamento non ecceda le finalità per le quali i dati sono raccolti o successivamente trattati e che sia temporalmente limitato.

Con riguardo al **principio di liceità** del trattamento, il trattamento è lecito se l'interessato ha espresso il suo consenso al trattamento o se esso è necessario per l'esecuzione di un contratto, l'adempimento di un obbligo legale, la salvaguardia di interessi vitali per una persona fisica, l'esecuzione da parte del Titolare di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o il perseguimento di un legittimo interesse ove non prevalgano i diritti e le libertà del soggetto interessato .

Principio di Responsabilizzazione.

Il principio di accountability (responsabilità) costituisce il valore aggiunto dell'intero corpo di norme contenute nel Regolamento e produce il passaggio da un approccio alla materia di tipo essenzialmente formalistico (basato sulla necessità di dovere compiere una serie di adempimenti, di per sé non sempre sinonimi di una concreta protezione dei dati trattati) ad un approccio finalizzato all'adozione di politiche aziendale (misure tecniche, organizzative e politiche) tali da raggiungere due scopi: 1. rendere effettiva la protezione dei dati personali; 2. dimostrarne la reale applicazione.

2. I criteri di liceità del trattamento

L'articolo 6 stabilisce i criteri di liceità del trattamento, ulteriormente specificati con riferimento alle circostanze relative all'equilibrio degli interessi, rispetto degli obblighi giuridici e all'interesse pubblico.

Condizioni richieste, alternativamente, perché il trattamento dei dati personali debba considerarsi lecito sono le seguenti:

a) espressione del consenso, esplicito e specifico;
b) esecuzione di un contratto di cui l'interessato sia parte;
c) adempimento di un obbligo legale in capo al Titolare;
d) salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
e) trattamento necessario per l'esecuzione di un compito di interesse pubblico. Possano essere considerati interessi pubblici alcuni "*interessi generali*», cioè comuni alla generalità delle persone appartenenti a un certo insieme costituente il gruppo di riferimento di un pubblico potere e che non potrebbero essere soddisfatti individualmente. (Ad es: salute pubblica, ordine pubblico, ecc.);
f) trattamento reso necessario dalla esigenza di tutelare un interesse legittimo del Titolare o di un terzo, sempre che non sussista un interesse o un diritto prevalente dell'interessato. Per le Autorità pubbliche che agiscono in esecuzione di un loro compito istituzionale, questa condizione non si applica.

I singoli Stati membri possono prevedere ulteriori specifiche in riferimento ai trattamenti di cui alle lettere c) ed e). Comunque, detti trattamenti devono essere disciplinati da una norma comunitaria o di uno Stato membro.

Qualora il trattamento abbia luogo per adempiere un obbligo legale oppure per eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, la base che legittima il trattamento dei dati personali deve avere come fondamento il diritto comunitario oppure quello di uno Stato membro.

3. I principi di privacy by design e privacy by default

L'art. 25 impone ai Titolari e ai Responsabili del trattamento dei dati obblighi di protezione fin dalla progettazione e di protezione di *default* (c.d. *data protection by design and by default*), richiedendo – tenuto conto della tecnologia

disponibile e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, così come della probabilità e della gravità del rischio derivante dal trattamento per i diritti e le libertà delle persone fisiche – l'adozione di misure tecniche e organizzative adeguate all'attività del trattamento e dei suoi obiettivi, quali la minimizzazione e la pseudonimizzazione dei dati. Ciò, al fine di tutelare i diritti dell'interessato nonché garantire che siano trattati, di *default*, solo i dati personali necessari per ogni specifica finalità del trattamento.

4. Organigramma aziendale privacy

Così come esiste un organigramma aziendale tout court andrà formalizzato un organigramma aziendale privacy che dovrà prevedere le seguenti figure:

- un **Titolare del trattamento** (persona giuridica Asl, nella persona del suo rappresentante legale);
- una serie di soggetti (persone fisiche) designati dal Titolare con la denominazione di "**Soggetti autorizzati al trattamento dei dati personali, con delega**", si tratta di coloro che in vigenza del Codice in materia di protezione dei dati personali – d.lgs. n. 196/2003 e s.m.i. - venivano designati con la dicitura di "Responsabili interni del trattamento dei dati personali"; in prima battuta, suddetta nomina riguarderà il Direttore Amministrativo, il Direttore Sanitario, i Direttori di Dipartimento, i Dirigenti Responsabili di UOC e, se ritenuto pertinente, alcuni Dirigenti di UOSD/UOS.

La dicitura "con delega" (riferita ai Soggetti autorizzati al trattamento dei dati personali) **sta a significare che essi dovranno** – ricorrendone i presupposti, in relazione ai trattamenti di dati di loro competenza e dopo averlo concordato con il Titolare – **nominare**:

a) in presenza di contratti di fornitura di prodotti e servizi in corso di esecuzione o da stipulare, aventi ad oggetto il trattamento di dati personali, **il Fornitore** (del prodotto o del servizio) **quale Responsabile del trattamento**, verificando l'attuazione delle misure tecniche e organizzative, da parte del fornitore stesso;
b) inoltre, **spetterà loro la nomina dei dipendenti, propri collaboratori** (quelli che ai sensi del d.lgs. n. 196/2003 e s.m.i. erano designati Incaricati del trattamento), **"soggetti autorizzati al trattamento dei dati personali" (si tratta esclusivamente di persone fisiche).**

I profili di responsabilità in capo ai "soggetti autorizzati al trattamento con delega"

Da ciò consegue che in applicazione del Regolamento **sono aumentati i profili di responsabilità** in capo ai "soggetti autorizzati al trattamento con delega" che risponderanno delle nomine che faranno nei confronti dei Fornitori (i quali saranno nominati Responsabile del trattamento) oltre che degli obblighi generali e di sicurezza del trattamento in capo a suddetti responsabili del trattamento.

Le nomine di cui ai punti a) e b) avverranno previa trasmissione da parte dell'Ufficio Privacy aziendale dell'apposita modulistica e di ulteriori informazioni in merito, entro la prima quindicina del mese di settembre c.a..

Può verificarsi il caso che il trattamento dei dati personali della ASL sia svolto da soggetti terzi; si pensi a chi effettua la manutenzione di apparecchiature diagnostiche che archiviano dati, al sistema RISPACS (impiegato per gestire tutte le attività amministrative e diagnostiche in un unico sistema, dall'accettazione all'esame, dalla refertazione all'archiviazione digitale del referto e delle immagini) al gestionale in uso presso la UOC di Laboratorio Analisi. Oppure a chi fornisce programmi e/o applicativi software (ad es, gestionale dei ricoveri, delle buste paga, della contabilità,, ecc.; oppure ancora a soggetti terzi presenti in Asl in qualità di Consulenti, di Associazioni di volontariato, ecc.

Tali soggetti saranno nominati Responsabile del trattamento dei dati personali dai Soggetti autorizzati al trattamento con delega.

- Ulteriore categoria riguarda i **soggetti autorizzati al trattamento dei dati personali** che sono nominati dai Soggetti autorizzati con delega che, appunto, nomineranno i propri collaboratori che trattano dati personali nello svolgimento della propria attività istituzionale.

Riassumendo avremo i seguenti profili:

interni alla ASL Lanciano – Vasto – Chieti:

Titolare	ASL n. 2
Soggetti autorizzati con delega	il Direttore Amministrativo, il Direttore Sanitario, i Direttori di Dipartimento, i Dirigenti Responsabili di UOC e, se ritenuto pertinente, alcuni Dirigenti di UOSD/UOS
Soggetti autorizzati	sono i dipendenti della Asl n. 2 nominati dai Soggetti autorizzati con delega, in base alla UOC/UOSD/UOS di appartenenza

esterni alla ASL Lanciano – Vasto – Chieti:

Responsabili del trattamento	nominati dai Soggetti autorizzati con delega

5. Portabilità dei dati

Nel Regolamento viene introdotto il diritto alla "portabilità" dei propri dati personali per trasferirli da un titolare del trattamento a un altro titolare. La norma fa eccezione nei casi i cui si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi. In questo caso il diritto non potrà essere esercitato, così come è vietato il trasferimento di dati personali verso Paesi extra Ue o organizzazioni internazionali che non rispondono agli standard di sicurezza in materia di tutela.

6. Il principio di "responsabilizzazione"

E' stata introdotta la responsabilizzazione dei titolari del trattamento (accountability) e un approccio che tenga in maggior considerazione i rischi che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Va precisato che, a differenza di quanto stabilito dalla Direttiva 95/46/CE la quale introduceva una distinzione tra **misure di sicurezza minime ed idonee**, l'applicazione di misure di sicurezza è finalizzata alla messa in sicurezza della organizzazione (la ASL), ciò significa che la conformità non garantisce la sicurezza mentre è vero il contrario, cioè che la sicurezza rende compliance (conforme) le misure predisposte.

La adozione di **misure tecniche ed organizzative** deve avvenire all'interno di un processo di miglioramento continuo, il che comporta in capo al Titolare l'obbligo di intervenire ogni qual volta ciò si renda necessario (ad es. perché è cambiata la normativa o perché sono intervenute nuove tecnologie che vanno ad impattare sui trattamenti in essere, oppure, perché si implementano nuovi trattamenti, oppure ancora, perchè c'è un ricambio di personale in un determinati Ufficio/UO/Ambulatorio).

Il principio di accountability (responsabilità) costituisce il valore aggiunto dell'intero corpo di norme contenute nel Regolamento e produce il passaggio da un approccio alla materia di tipo essenzialmente formalistico (basato sulla necessità di dovere compiere una serie di adempimenti, di per sé non sempre sinonimi di una concreta protezione dei dati trattati) ad un approccio finalizzato all'adozione di politiche aziendale (misure tecniche, organizzative e politiche) tali da raggiungere due scopi: 1. rendere effettiva la protezione dei dati personali; 2. dimostrarne la reale applicazione.

7. Data breach

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali al Garante entro **settantadue ore** dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il titolare **potrà decidere di non informare gli interessati** se riterrà che la violazione non comporti un rischio elevato per i loro diritti oppure se dimostrerà di avere già adottato misure di sicurezza; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato al rischio. In questo ultimo caso dovrà provvedere con una comunicazione pubblica.

L'Autorità Garante **potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria valutazione dei rischi correlati alla violazione commessa.**

Rispondere in modo efficace a una violazione dei dati richiede un approccio multidisciplinare ed integrato con il coinvolgimento di diverse funzioni aziendali di volta in volta coinvolte.

Il primo adempimento da porre in essere per la Asl è l'**adozione del Registro dei trattamenti di dati personali**, ma prima ancora, **i dipendenti devono comprendere l'importanza e il valore dei dati,** nonché gli ingenti **danni economici legati a una perdita di informazione.**

Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare i danni.

8. La figura del Responsabile della Protezione dei dati / DPO (Data Protection Officer)

E' stata prevista la figura del "Responsabile della protezione dei dati" (Data Protection Officer o DPO), **incaricato di assicurare una gestione corretta dei dati personali** nelle imprese e negli enti. Egli è individuato in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati.

La Asl di Lanciano – Vasto - Chieti, soggetto obbligato a suddetta nomina, ha nominato in qualità di Responsabile per la protezione dei dati il dott. Giovanni Modesti, cui si forniscono i dati di contatto:
Dott. Giovanni Modesti
c/o UOC Affari Generali e Legali
Email: dpo@asl2abruzzo.it
PEC: dpo@pec.asl2abruzzo.it
Tel. 358074

Il Responsabile della protezione dei dati:

➢ **riferisce direttamente al vertice aziendale,**
➢ **è' indipendente,** non riceve istruzioni per quanto riguarda l'esecuzione dei compiti;
➢ deve avere una specifica competenza "della normativa e delle prassi in materia di dati personali nonché delle norme e delle procedure amministrative che caratterizzano il settore";
➢ **deve,** inoltre, **avere** anche **"qualità professionali adeguate alla complessità del compito da svolgere"** e, specialmente con riferimento a settori delicati come quello della **sanità**, deve dimostrare di avere anche competenze specifiche rispetto ai tipi di trattamento posti in essere al titolare;
➢ **gli va garantita l'autonomia decisionale** e la **sua estraneità rispetto alla determinazione delle finalità e delle modalità del trattamento dei dati.**

Il responsabile della protezione dei dati svolgei seguenti compiti:

a) **informa e fornisce consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti** che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) **sorveglia l'osservanza del Regolamento,** 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) **fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati** e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) **coopera con l'autorità di controllo;** e
e) **funge da punto di contatto per l'autorità di controllo 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.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

9. I diritti del cittadino

I cittadini riguardo al trattamento dei propri dati personali vantano una serie di diritti che si vanno di seguito ad elencare.

Diritto al rilascio della informativa
Attraverso la Informativa, vanno fornite all'interessato notizie relative al:

- Titolare (identità + dati di contatto),
- Responsabile, (solo dati di contatto),
- rappresentante (se è stato individuato);
- finalità del trattamento, con relativo riferimento normativo;
- se il trattamento è svolto per l'esercizio di un legittimo interesse del Titolare o di un terzo, quale sia il legittimo interesse; gli eventuali destinatari dei dati personali;
- l'intenzione, eventuale, di trasferire i dati trattati in un Paese terzo e la presenza o l'assenza di una decisione di adeguatezza della Commissione.

A corredo di tali informazioni, sempre al fine di rendere più trasparente l'intero procedimento, vanno fornite ulteriori informazioni relativamente ai seguenti aspetti:

- periodo di conservazione,
- diritti in capo all'interessato,
- diritto di revocare il consenso;
- diritto di proporre reclamo ad una Autorità di controllo;
- se la comunicazione dei dati è legata ad un obbligo di natura contrattuale o legale;
- se al trattamento è connesso un processo decisionale automatizzato.

Diritto alle tutele sulla prestazione del consenso

La prestazione del consenso è il primo atto di partecipazione attiva dell'utente e rappresenta l'accettazione, non obbligatoria, al trasferimento e trattamento dei dati. Il consenso deve essere espresso mediante un atto positivo inequivocabile, libero e specifico. Non è vincolante il mezzo, potendo comunicarlo in forma scritta, mediante mezzi elettronici o oralmente.

Ai fini di una valutazione della libertà del consenso particolare attenzione dovrà essere posta ai dati personali che vengono richiesti ed alla correlazione rispetto alla prestazione. Può capitare, infatti, che la richiesta di consenso per l'esecuzione di un contratto sia condizionata dall'autorizzazione al trattamento di dati non necessari. In casi come questi viene pregiudicata proprio la libertà del consenso manifestato dal cittadino nonché la violazione del principio di minimizzazione dei dati ossia il criterio secondo cui i dati richiesti devono essere adeguati, pertinenti e limitati rispetto alla finalità per la quale sono richiesti.

Tenuto conto che i dati rappresentano il cittadino/utente e continuano a rappresentarlo anche durante e dopo il trattamento, occorre che, già all'atto della prestazione del consenso, questi sia debitamente informato delle garanzie che saranno adoperate per tutelare i dati nonché dei diritti che ha di accedere, di intervenire per controllare il trattamento (ad esempio presentando un eventuale reclamo), o di rettificare o anche ritirare il consenso.

Diritto al divieto di trattare alcune categorie di dati personali

Il divieto di trattare alcune categorie di dati personali nasce dalla semplice considerazione che i dati non sono tutti uguali. Le informazioni che riguardano la persona non hanno tutte lo stesso peso e lo stesso valore.

Ci sono, effettivamente, dati strumentali alla richiesta di attivazione di determinati servizi o contratti per i quali all'utente sarà sottoposto un modulo per fornire il consenso, e dati che non hanno, per loro stessa natura, alcun ruolo nella stipula di nuovi contratti. Per il primo tipo di dati indicati, il controllo che potrà essere fatto sull'operato del titolare del trattamento, nel momento in cui viene richiesto il consenso, sarà di tipo funzionale ed orientato a rispetto del **principio della minimizzazione** dei dati raccolti.

Accanto a queste informazioni, **vi sono poi categorie di dati, relative alla persona, per le quali vige il divieto di trattamento, superabile solo nel caso in cui vi sia un consenso esplicito prestato per assolvere a diritti e/o obblighi specifici, per tutelare interessi vitali (salute) o anche, tra l'altro, nel caso in cui sia l'interessato a renderli di dominio pubblico.**

Questi dati, che godono di particolare tutela, sono quelli inerenti l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, **i dati genetici, biometrici, relativi alla salute o alla vita sessuale o all'orientamento sessuale**. Per il trattamento di dati relativi a condanne penali occorre il controllo della pubblica autorità.

Diritto di accesso dell'interessato

Il diritto di accesso dell'interessato è strettamente connesso alla durata del trattamento dei dati scaturente dal consenso prestato. Esso sancisce il rapporto indissolubile tra utente e dati personali per cui **la persona interessata ha sempre il diritto di ottenere dal titolare del trattamento la conferma che vi sia in corso un trattamento dei propri dati** e, in caso positivo, accedere alle informazioni inerenti lo specifico trattamento, ossia **sapere per quali fini sono stati adoperati i dati, quali dati sono stati adoperati, a chi sono stati comunicati, il periodo di tempo entro cui i dati saranno conservati o una previsione della durata, la possibilità di esercitare i diritti di rettifica, cancellazione o di limitazione all'uso dei dati, o anche il rifiuto del trattamento, così come il diritto di proporre reclamo presso il Garante per la protezione dei dati.**

Il diritto di accesso rappresenta, proprio per il potere che conferisce all'utente, una porta aperta sull'operato del titolare del trattamento riconoscendo il grande potere, ad ogni persona fisica, di controllare nel tempo le tracce lasciate dai propri dati e di intervenire, eventualmente, per cambiare le cose.

In sintesi è come se venisse riconosciuto il potere di controllare le conseguenze del consenso prestato e di correggerlo o di cancellarlo, come pure solo di monitorarlo ottenendo le informazioni richieste, ricordando che quei dati sono e restano dell'interessato.

Per accedere a queste informazioni, occorre che il titolare del trattamento riscontri la richiesta. In capo allo stesso si configura, pertanto, il dovere di fornire le informazioni.

Dovere di fornire le informazioni richieste

Il dovere di fornire le informazioni richieste è strettamente collegato alla richiesta del cittadino formulata nell'esercizio del diritto di accesso e rappresenta il riscontro che il titolare del trattamento (ASL Lanciano – Vasto - Chieti) ha il dovere di fornire all'interessato senza alcun aggravio economico, salvo il caso in cui risultino manifestamente infondate o eccessive.
Quanto alla tempistica è stato fissato un **termine massimo di un mese, prorogabile a due mesi nei casi di complessità o di elevato numero di richieste**. Se non dovesse rispettarla, vengono ad attivarsi ulteriori diritti di azione riconosciuti all'interessato.

Possibilità di proporre reclamo/ricorso
La possibilità di proporre reclamo/ricorso è riconosciuta al cittadino nel caso in cui il titolare del trattamento non riesca a fornire le informazioni richieste dall'interessato.
Infatti, decorso il tempo di un mese o più, in caso di proroga, il titolare del trattamento dovrà comunque informare delle sue difficoltà a fornire tempestivo riscontro, nonché della possibilità per il cittadino di adire, con reclamo, il Garante per la protezione dei dati personali oppure, con ricorso, l'autorità giurisdizionale (giudice ordinario).

Diritto di rettifica
Il diritto di rettifica potrà essere esercitato ogni qualvolta l'interessato (la persona cui appartengono i dati) riscontri l'utilizzo di dati personali inesatti.
L'inesattezza dei dati posseduti dal titolare del trattamento è un'ipotesi che può verificarsi molto più frequentemente di quanto non si pensi e che può avere anche conseguenze rilevanti per il cittadino. Da qui la necessità di riconoscere agli utenti il diritto ad ottenere la rettifica dei dati, al fine di evitare che l'errore possa danneggiarli o, comunque, avere conseguenze negative.
Ovviamente se viene riconosciuto il diritto di chiedere la rettifica, al fine di rendere efficace la richiesta, occorre che alla stessa il titolare del trattamento dia seguito senza ingiustificato ritardo. Qualora la richiesta avesse ad oggetto l'integrazione di dati incompleti, potrà essere fornita una dichiarazione integrativa.

Revoca del consenso
La revoca del consenso non è sottoposta ad alcun vincolo o condizione né di carattere temporale né di natura strutturale. Così come viene garantita la possibilità di esprimere un consenso "libero", il Regolamento garantisce il diritto di revocare il consenso con la stessa "libertà".
Il diritto di revocare il consenso è, pertanto, esercitabile in qualsiasi momento. Ovviamente il trattamento dei dati avvenuto nell'arco di tempo coperto dal consenso espresso, resta lecito. Inoltre, occorre che non siano stabilite modalità di revoca del consenso più articolate (finalizzate a disincentivare la revoca) rispetto a quelle di prestazione dello stesso.
Di ciò, ossia del diritto di revocare il consenso, il cittadino deve avere notizia (mediante la Informativa) già nel momento stesso in cui presta il consenso.

Diritto all'oblio
La finalità principale di questo diritto riconosciuto all'utente è stretta conseguenza dell'uso di tecnologie sempre più avanzate che potrebbero compromettere l'immagine dell'utente continuando, ad esempio, a diffondere dati in violazione del consenso, in quanto revocato, oppure perché il trattamento dei dati è avvenuto illecitamente.
Ai sensi dell'art. 17, paragrafo 3, lett. c), il diritto all'oblio non può essere esercitato dall'utente "per motivi di interesse pubblico nel settore della sanità pubblica (omissis)". Pertanto, non si applica in relazione ai dati personali trattati dalla ASL LANCIANO – VASTO - CHIETI.

Diritto di limitazione del trattamento
Il diritto di limitazione del trattamento è attivabile dal cittadino ogni qualvolta vi sia una situazione da verificare o un conflitto tra interessato e titolare del trattamento.
Al fine di evitare che questo tempo di sospensione necessario per dirimere l'eventuale controversia possa, pur esso, rappresentare un ulteriore aggravio per il cittadino, si è ritenuto opportuno creare una sorta di "sospensione" per mezzo della quale si opera una limitazione temporale del trattamento in attesa di conoscere la sorte dei dati.
L'interessato può chiedere al titolare del trattamento, ed ha il diritto di ottenerla, una limitazione di uso dei dati. La sua portata è più estesa rispetto al semplice "blocco" del trattamento potendo, la richiesta, essere motivata facendo riferimento ad una contestazione sull'esattezza dei dati, su un ipotizzato trattamento illecito o anche perché ci si è opposti al trattamento.

Diritto alla portabilità dei dati
Il diritto alla portabilità dei dati è predisposto, funzionalmente, sul riconoscimento del diritto del cittadino di trasmettere i propri dati, forniti ad un titolare del trattamento, ad altro titolare.

Ai sensi dell'art. 20, paragrafo 3 il diritto alla portabilità non può essere esercitato dall'utente che ha fruito dei servizi sanitari da parte della ASL LANCIANO – VASTO - CHIETI.

Diritto di opporsi al trattamento dei dati personali

Il diritto di opporsi al trattamento dei dati personali può essere esercitato dal cittadino in qualsiasi momento.
Non vi sono motivi particolari che devono essere addotti alla base della richiesta, ricevuta la quale, al titolare del trattamento non resterà altro da fare che astenersi dal trattare ulteriormente i dati, a meno che non dimostri l'esistenza di motivi legittimi cogenti che prevalgono su quelli dell'interessato.
Anche questo diritto dell'interessato deve essere comunicato in sede di richiesta iniziale del consenso, rappresentando il potere di modificare nel tempo l'autorizzazione concessa col consenso e, pertanto, dando immediatamente contezza, all'utente, della possibilità non solo di rivedere il consenso ma anche di opporsi al trattamento dei dati per motivi semplicemente connessi alla sua situazione particolare.

10. I poteri dell'autorità di controllo (Garante privacy)

All'autorità di controllo, in Italia è il Garante Privacy, sono conferiti poteri di indagine, correttivi, autorizzativi e consultivi, oltre al potere di infliggere sanzioni amministrative pecuniarie.
Tali poteri possono esercitati direttamente dal Garante o, indirettamente, con l'ausilio del Nucleo Speciale della Guardia di Finanza.
Ecco che c'è da sapere sui poteri del Garante privacy nel Regolamento.

11. Sanzioni amministrative per violazioni del Regolamento

Il Regolamento distingue due tipologie di sanzioni amministrative in base al loro ammontare (10 o 20 milioni di euro).

Sanzioni amministrative fino a 10 milioni di euro, o in caso di un'impresa, fino al 2% del fatturato totale annuo mondiale, se superiore.

Ci si riferisce alle violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui ai seguenti articoli:

• art. 8	• (consenso dei minori),
• art. 10	• (trattamenti che non richiedono l'identificazione degli interessati),
• art. 23	• (privacy by design e privacy by default),
• art. 24	• (contitolarità del trattamento),
• art. 25	• (nomina rappresentante del Titolare non stabilito nell'Unione Europea),
• art. 26	• (Responsabili del trattamento),
• art. 27	• (istruzioni e autorità del Titolare),
• art. 28	• (documentazione relativa a ciascun trattamento di dati personali),
• art. 29	• (cooperazione con l'Autorità di vigilanza),
• art. 30	• (sicurezza del trattamento),
• art. 31	• (notificazione dei data breach al Garante),
• art. 32	• (comunicazione dei data breach agli interessati),
• art. 33	• (DPIA – Data Protection Impact Assessment),

• art. 34	• (consultazione preventiva dell'Autorità di vigilanza),
artt. 35, 36 e 37	(valutazione d'impatto sulla protezione dei dati e consultazione preventiva)
• art. 39	• (compiti del Responsabile della protezione dei dati)
• art. 40	• (processi di certificazione).

Sanzioni amministrative fino a 20 milioni di euro, o in caso di un'impresa, fino al 4% del fatturato totale annuo mondiale.

Ci si riferisce alle violazioni delle disposizioni relative agli obblighi del Titolare o del Responsabile di cui ai seguenti articoli:

• art. 5 e ss.	• (principi base del trattamento)
• art. 7 e ss.	• (condizioni per il consenso)
• art. 12 e ss.	• (diritti degli interessati)
• artt. 44 e ss.	• (trasferimento di dati personali all'estero)
• art. 58	• (mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'Autorità di vigilanza).

12. Sanzioni penali per la violazione al Regolamento

Le sanzioni penali rimangono di competenza di ogni singolo Stato, che deve predisporre sanzioni "effettive, proporzionate e dissuasive".

1. 13. Le responsabilità e le sanzioni

Chi risponde delle violazioni

Nella individuazione del soggetto a cui imputare un profilo di responsabilità, si dovrà operare **in base alla legge n. 689/1981** la quale prevede che **la notificazione del verbale** (redatto dall'Autorità Garante della Privacy o dal Nucleo Speciale della Guardia di Finanza) **venga effettuata nei confronti del contravventore e del responsabile in solido,** purchè quest'ultima figura sia stata formalmente designata e siano state riscontrate anche inadempienze gravi imputabili a tale ruolo.

Inoltre, l'art. 3 della legge n. 689/1981 prevede che la violazione amministrativa sia applicata anche qualora ricorra solo la colpa dell'agente, questo ha risvolti particolarmente rilevanti sul piano operativo.

Mentre l'art. 167 del vecchio Codice in materia di protezione dei dati personali (d.lgs. n. 196/2003) disciplinava il trattamento illecito come un reato a dolo specifico e richiedeva anche il nocumento (danno patrimoniale apprezzabile), con il Regolamento questi due elementi non sono necessari affinché ricorra la violazione amministrativa.

Con il Regolamento, è sufficiente che manchi l'informativa o il consenso o che il consenso prestato non abbia i requisiti di legge perché venga applicata la violazione amministrativa.

A tale riguardo diversi articoli del Regolamento europeo rafforzano gli obblighi generali e di sicurezza del trattamento in capo al responsabile del trattamento (che è un soggetto esterno alla ASL LANCIANO – VASTO - CHIETI) e/o al "soggetto autorizzato al trattamento dei dati personali con delega" (che è un dipendente della ASL LANCIANO – VASTO - CHIETI), dagli articoli 28 e 30 all'art. 33 sulla notificazione della violazione dei dati, infine, l'articolo 83, lettera d) dando rilevanza al grado di responsabilità tra titolare e responsabile rende esplicita l'attribuzione anche al responsabile dell'illecito amministrativo.

14. Riferimenti

http://www.garanteprivacy.it/web/guest/regolamentoue

Il Responsabile della protezione dei dati
Dott. Giovanni Modesti