# Nuove regole sulla Privacy

Le principali novità del Nuovo Regolamento sono le seguenti.

**Liceità del trattamento dei dati e condizioni per la manifestazione del consenso**

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Il consenso deve essere esplicito per i dati "sensibili", fra i quali vi sono i dati relativi allo stato di salute.

Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

Deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

**L’informativa**

Il titolare deve sempre specificare la base giuridica del trattamento, cioè la motivazione alla base della raccolta dei dati.

Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione e il diritto di presentare un reclamo all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

**Contenuti dell’informativa**

I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **DEVE SEMPRE** specificare i **dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer)**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).

Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

**Tempi dell'informativa**

Nel caso di dati personali non raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**NON** della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

**Modalità dell'informativa**

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee *(si veda anche considerando 58)*.

L'informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: *si vedano art. 12, paragrafo 1, e considerando 58*), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** *(art. 12, paragrafo 7)*; queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea

Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** *(si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo)*, anche se occorre sottolineare che **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** *(si veda art. 14, paragrafo 5, lettera b) )* – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

L'informativa *(disciplinata nello specifico dagli artt. 13 e 14 del regolamento)* deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano**, le **finalità del trattamento**, i **diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

**NOTA**: ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

E' opportuno che i titolari di trattamento **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento.

Il regolamento supporta chiaramente il concetto di **informativa "stratificata"**, più volte esplicitato dal Garante nei suoi provvedimenti [si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 relativo all'utilizzo di un'icona specifica per i sistemi di videosorveglianza con o senza operatore; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675 contenente prescrizioni analoghe rispetto all'utilizzo associato di sistemi biometrici e di videosorveglianza in istituti bancari], in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove **l'utilizzo di strumenti elettronici** per garantire la massima diffusione e semplificare la prestazione delle informative.

I titolari potranno, dunque, una volta adeguata l'informativa nei termini sopra indicati, **continuare o iniziare a utilizzare queste modalità** per la prestazione dell' informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) – in attesa della definizione di icone standardizzate da parte della Commissione.

Dovranno essere adottate anche le **misure organizzative interne** idonee a garantire il rispetto della tempistica: il termine di 1 mese per l'informativa all'interessato è chiaramente un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a), del regolamento menziona in primo luogo che il **termine deve essere "ragionevole"**.

Poiché spetterà al titolare valutare lo **sforzo sproporzionato** richiesto dall'informare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del regolamento, sarà utile fare riferimento ai **criteri evidenziati nei provvedimenti** con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione (si veda, in particolare, il provvedimento del 26 novembre 1998 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39624; più di recente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423 in tema di esonero dagli obblighi di informativa).

**La nomina del Responsabile della Protezione dei Dati (RPD)**

Una delle novità più importanti del Regolamento Europeo è la nomina di un Responsabile della Protezione dei Dati (RPD in italiano, DPO in inglese).

Questo soggetto deve essere in possesso di adeguate capacità professionali, in particolare, della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati personali e ha il compito di aiutare a mantenersi conformi alle nuove regole sulla protezione della privacy.

Il DPO funge anche da intermediario con le autorità di controllo, in particolare l'autorità giudiziaria ed il Garante della Privacy.

La nomina del RPD è obbligatoria per tutti gli Enti Pubblici, nonché per le attività il cui esercizio comporta la manipolazione di dati in "larga scala" per speciali categorie di dati, tra i quali i dati sanitari. **Per gli studi medici tale nomina non è obbligatoria**, anche se tutti i commentatori la consigliano vivamente per supportare il titolare dello studio nell'adempimento degli obblighi sulla privacy.

La funzione di RPD può essere svolta da un fornitore esterno di servizi purché sia esercitata sulla base di un contratto stipulato tra il titolare dello studio ed una persona fisica oppure giuridica, quindi una società. Per fare un esempio: lo studio medico delega la responsabilità al fornitore del proprio software gestionale (attraverso un accordo sul trattamento dei dati), che nominerà un RPD per tutti i dati contenuti nei propri server e gestiti attraverso il software. Ma occorre fare attenzione, poiché questo sarà possibile solo nel caso in cui il gestionale sia un software in cloud, dato che la tecnologia cloud permette di controllare da remoto tutti i dati dello studio. Per tutti gli altri eventuali dati che lo studio conserva fisicamente sui propri dispositivi (o in cartaceo), invece, il titolare dello studio deve conformarsi alle norme sancite dal Regolamento sotto la propria responsabilità, eventualmente nominando il RPD.

**Laddove si rendesse obbligatoria la nomina del Responsabile della protezione dei dati (DPO) l'art. 37, ultimo comma, del Nuovo Regolamento 679/2016, prevede che il titolare del trattamento (il medico), pubblichi i dati di contatto del DPO e li comunichi all'autorità di controllo (Garante). Il modello di comunicazione è riportato nell'apposito link.**

**Compiti del DPO**

Secondo le nuove FAQ del Garante (vedi link), il DPO deve assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento, coopera con l'Autorità e

costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

**INFORMAZIONE**
**GENTILI SIGNORI,**
**DESIDERO INFORMARVI CHE I VOSTRI DATI SONO UTILIZZATI SOLO PER SVOLGERE ATTIVITÀ NECESSARIE PER PREVENZIONE, DIAGNOSI, CURA, RIABILITAZIONE O PER ALTRE PRESTAZIONI DA VOI RICHIESTE, FARMACEUTICHE E SPECIALISTICHE.**
**SI TRATTA DEI DATI FORNITI DA VOI STESSI O CHE SONO ACQUISITI ALTROVE, MA CON IL VOSTRO CONSENSO, AD ESEMPIO IN CASO DI RICOVERO O DI RISULTATI DI ESAMI CLINICI.**
**ANCHE IN CASO DI USO DI COMPUTER, ADOTTO MISURE DI PROTEZIONE PER GARANTIRE LA CONSERVAZIONE E L'USO CORRETTO DEI DATI ANCHE DA PARTE DEI MIEI COLLABORATORI, NEL RISPETTO DEL SEGRETO PROFESSIONALE.**
**SONO TENUTI A QUESTE CAUTELE ANCHE I PROFESSIONISTI** (IL SOSTITUTO, IL FARMACISTA, LO SPECIALISTA) **E LE STRUTTURE** (LABORATORIO ANALISI, AZIENDE OSPEDALIERE, CASE DI CURA PRIVATE) **CHE POSSONO CONOSCERLI E CHE IN ACCORDO CON LEI SEGUIRANNO IL PERCORSO DIAGNOSTICO TERAPEUTICO ASSISTENZIALE.**
**I DATI NON SONO COMUNICATI A TERZI, TRANNE QUANDO SIA NECESSARIO O PREVISTO DALLA LEGGE.**
**SI POSSONO FORNIRE INFORMAZIONI SULLO STATO DI SALUTE A FAMILIARI E CONOSCENTI SOLO SU VOSTRA INDICAZIONE.**
**IN QUALUNQUE MOMENTO POTRETE CONOSCERE I DATI CHE VI RIGUARDANO, SAPERE COME SONO STATI ACQUISITI, VERIFICARE SE SONO ESATTI, COMPLETI, AGGIORNATI E BEN CUSTODITI, E FAR VALERE I VOSTRI DIRITTI AL RIGUARDO.**
**PER ATTIVITÀ PIÙ DELICATE DA SVOLGERE NEL VOSTRO INTERESSE, SARÀ MIA CURA INFORMARVI IN MODO PIÙ PRECISO.**

**La presente informativa verrà aggiornata dopo il 24 maggio 2018, tenuto conto che a decorrere dal 25 maggio 2018 sarà applicabile il Regolamento (UE) 2016/679**