NUOVO REGOLAMENTO EUROPEO TRATTAMENTO DATI PERSONALI - COSA CAMBIA E PER CHI !

SOMMARIO

A CHI SI APPLICA

Solo alle persone fisiche individuate o individuabili.

I TEMPI!

NORMATIVA ESSENZIALE

Il **4 maggio 2016**, sono stati pubblicati sulla gazzetta ufficiale dell'unione europea i testi del **regolamento europeo in materia di protezione dei dati personali** e della **direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini**.

Il **24 maggio** 2016 è entrato ufficialmente in vigore il regolamento, che diventerà definitivamente applicabile in via diretta in tutti i paesi dell'Unione a partire dal **25 maggio 2018**.
Entro quella data gli stati europei dovranno introdurla nel proprio paese con facoltà, di modificare alcune indicazioni (es. coordinamento sanzioni, modalità trattamento dati genetici, età per esprimere il consenso).

L'Italia con legge del 25 ottobre 2017, n. 163 ha delegato il governo ad adottare i criteri direttivi per l'applicazione della normativa e si è in attesa del decreto legislativo applicativo.

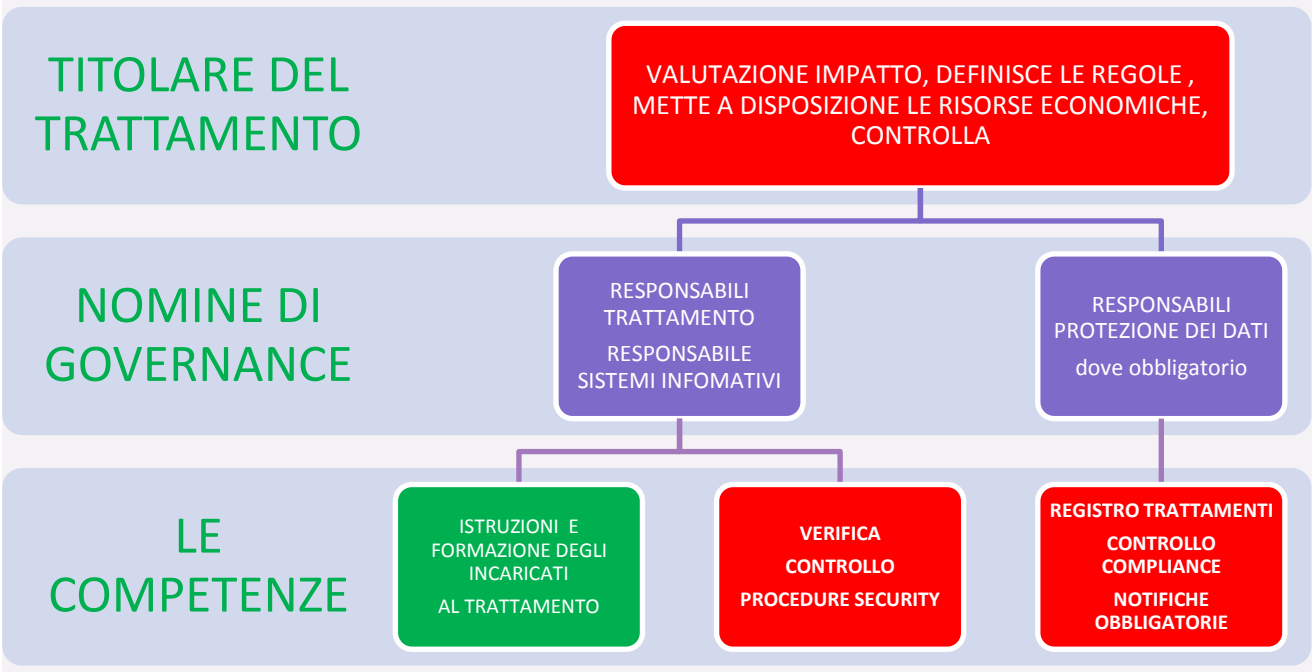
IL PRINCIPIO DI ACCOUNTABILITY

Il regolamento pone con forza l'accento sulla "**responsabilizzazione**" (cd accountability) di titolari e responsabili – ossia, sull'**adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.**

Il titolare del trattamento **(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)** dovrà dimostrare di avere messo in pratica ogni opportuna iniziativa di formazione e ogni attività di protezione ed informatica per proteggere i dati e le informazioni**.**

Nel caso di danno: al titolare spetterà dimostrare l'esistenza delle misure di sicurezza e che il danno si è verificato per cause fortuite (art. 2043 e 2050 codice civile).

In pratica:



QUANDO È OBBLIGATORIO NOMINARE UN RESPONSABILE PROTEZIONE DEI DATI (DATA PROTECION OFFICER)

Normativa essenziale:
Art 37-39 regolamento
linee-guida sui responsabili della protezione dei dati (rpd) - wp243 adottate dal

gruppo di lavoro art. 29 il 13 dicembre 2016

Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per **assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del regolamento medesimo.**

Coopera con l'autorità ed è obbligato alla comunicazione al Garante delle violazioni che possono comportare danni alle persone ai quali si riferiscono i dati.

Il Garante per la protezione di dati personali ha chiarito:

NO

- SINGOLO PROFESSIONISTA COMPRESI I MEDICI ANCHE IN FORMA ASSOCIATA, PEDIATRI, MEDICI SPECIALISTI SINGOLI
- FARMACIE
- AGENTI COMMERCO, MEDIATORI NON SU LARGA SCALA
- IMPRESE INDIVIDUALI O FAMILIARI
- PICCOLE E MEDIE IMPRESE
- **CON RIFERIMENTO AI TRATTAMENTI DEI DATI PERSONALI CONNESSI ALLA GESTIONE CORRENTE DEI RAPPORTI CON FORNITORI E DIPENDENTI**

SI

- AZIENDE CON PIU' DI 250 DIPENDENTI
- ENTI PUBBLICI
- ISTITUTI DI CREDITO
- IMPRESE ASSICURATIVo
- SISTEMI DI INFORMAZIONE CREDITIZIA E SOCIETÀ FINANZIARIE
- SOCIETÀ DI INFORMAZIONI COMMERCIALI
- SOCIETÀ DI REVISIONE CONTABILE E SOCIETÀ DI RECUPERO CREDITI
- ISTITUTI DI VIGILANZA
- AZIENDE CHE SI OCCUPANO DI CONTROLLO TELECAMERE TRAFFICO E/O A DISTANZA
- PARTITI E MOVIMENTI POLITICI
- SINDACATI, CAF E PATRONATI
- SOCIETÀ OPERANTI NEL SETTORE DELLE "UTILITIES" (TELECOMUNICAZIONI, DISTRIBUZIONE DI ENERGIA ELETTRICA O GAS)
- IMPRESE DI SOMMINISTRAZIONE DI LAVORO E RICERCA DEL PERSONALE
- SOCIETÀ OPERANTI NEL SETTORE DELLA CURA DELLA SALUTE, DELLA PREVENZIONE/DIAGNOSTICA SANITARIA QUALI OSPEDALI PRIVATI, TERME, LABORATORI DI ANALISI MEDICHE E CENTRI DI RIABILITAZIONE
- SOCIETÀ DI CALL CENTER; SOCIETÀ CHE FORNISCONO SERVIZI INFORMATICI
- SOCIETÀ CHE EROGANO SERVIZI TELEVISIVI A PAGAMENTO

Qualifiche professionali

- Non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi.
- Deve possedere un'approfondita conoscenza della normativa e delle prassi in materia

di privacy, **nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento**.

- Costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del regolamento).
- Il responsabile della protezione dei dati personali deve poter disporre, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

La nomina deve essere fatta in modo scritto.

Il suo nominativo andrà comunicato al garante in via telematica secondo le procedure che saranno indicate **per la comunicazione va utilizzato l'apposito modello** scaricabile dal sito del garante.

La pubblica amministrazione dovrà utilizzare per la nomina **lo schema indicato dal garante per la protezione dei dati**.

QUANDO È POSSIBILE TRATTARE DATI SENSIBILI

Ai sensi dell'art. 9 del regolamento sono dati sensibili quelli che identificano:

- origine razziale o etnica
- le opinioni politiche
- le convinzioni religiose o filosofiche
- appartenenza sindacale
- dati genetici
- dati biometrici intesi a identificare in modo univoco una persona fisica
- dati relativi alla salute o alla vita sessuale o all'orientamento sessuale

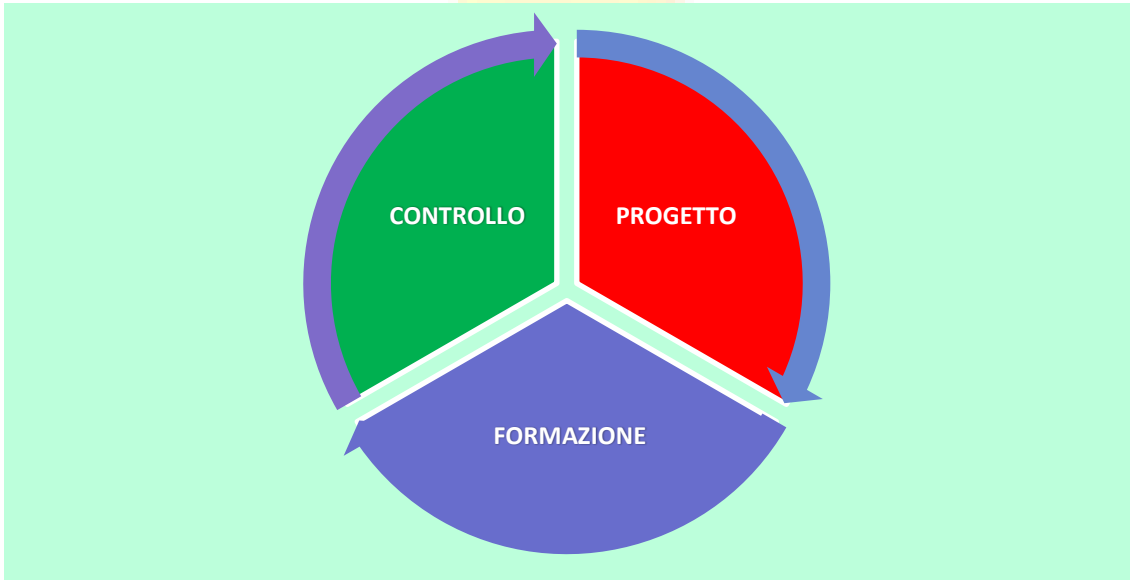
Possono essere trattati se l 'interessato ha prestato il consenso o il trattamento sia obbligatorio per legge. In particolare per :

- **Assolvere oneri di assistenza sociale**, lavorativa, previdenziale.
- **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.
- **Nell'ambito delle 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.

- **Dati personali resi manifestamente pubblici** dall'interessato.
- **Accertare, esercitare o difendere un diritto in sede giudiziaria** o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali.
- **Motivi di interesse pubblico rilevante.**
- **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.
- **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.
- **E' necessario a fini di archiviazione nel pubblico interesse,** di ricerca scientifica o storica o a fini statistici.

IN SINTESI!
LA SICUREZZA SI PROGETTA, SI INSEGNA E SI CONTROLLA



Responsabile Protezione Dati (dpo)	Enti pubblici Strutture private che trattano in gran quantità dati sensibili
Nomina responsabili trattamento dei dati	Analisi della struttura ed individuare persone che trattano una categoria particolare di dati (es. personale, dati sanitari) .
Indicazioni alle persone incaricate al trattamento	Non è più necessaria la lettera scritta ma è comunque opportuno farla per fornire ai dipendenti le regole minime di trattamento.
Formazione personale	Si – Tutti - in particolare quelli che trattano dati sensibili
Codice etico	Utile quando i dati sono condivisi tra più persone anche esterne alla struttura

Valutazione impatto

Si -Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "**possa presentare un rischio elevato**" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017

Il regolamento generale sulla protezione dei dati non richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4).

Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati .

Misure sicurezza minime

Tutti

- Analisi rischio
- Formazione personale
- Adozione programmi privacy designer
- Password d'accesso dati sensibili e profilazione criteri accesso
- Sistemi antintrusione per la protezione dei dati (antivirus, separazione dati sensibili dai comuni ecc.)
- Backup, disaster recovery
- Prove di ripristino
- Verifica conformità ed informative sistemi videosorveglianza e controllo a distanza

Analisi privilegi accesso	Si
Registro trattamento	Si – per le categorie sopra indicate
Valutazione della indispensabilità dei dati personali	Si
Analisi della struttura informatica	Si
Videosorveglianza e sistemi di controllo a distanza	Verifica misure sicurezza obbligatorie – Permessi uffici del lavoro nel caso di personale Informazioni al personale ed ai terzi obbligatorie
Valutazione software	Si – il software deve essere conformato "privacy designer". Ciò programmi già progettati per garantire alti standard di sicurezza
Tracciamento log	Si
Minimizzazione dati	Si
Anonimizzazione e/o pseudoanonimizzazione	Si – dati sensibili
Cifratura	Si
Valutazione termini di conservazione	Si
Controllo accesso ai dati	Si
Consenso al trattamento	Si per i dati sensibili – deve essere documentabile anche se non è piu' obbligatoria la sottoscrizione. Non è necessario richiedere il consenso se fatto prima
Informativa	Si
Rischio elevato dubbi	Nel caso di dati personali sensibili con rischio elevato le misure di sicurezza possono essere portate alla valutazione del garante
Denuncia degli accessi non autorizzati	Si – entro 72 ore nelle condizioni sopra indicate

Obbligo notifica garante	Abolito

Consenso al trattamento

Per i dati "sensibili" (si veda art. 9 regolamento) **il consenso**

DEVE essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione.

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); inoltre, il titolare (art. 7.1) DEVE essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

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. L'Italia opterà per i 14 anni); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Cosa non cambia?

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**" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.

In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica.

Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2).

I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20)

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 vecchi 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 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

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.

Esonero informativa

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.

Cosa non cambia?

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).