GDPR:

IL NUOVO REGOLAMENTO N. 679/2016 UE SULLA PROTEZIONE DEI DATI PERSONALI – GUIDELINES – REGOLE – IMPATTI - SANZIONI

Via S. Allende, 99 interno 1 - 47841 Cattolica (RN)
Cell. 328.3123467 - Mail margherita.patrignani@gmail.com
PEC margherita.patrignani@ordineavvocatirimini.it
P. Iva 04 008 510 408

Studio Legale

Avv. Margherita Patrignani

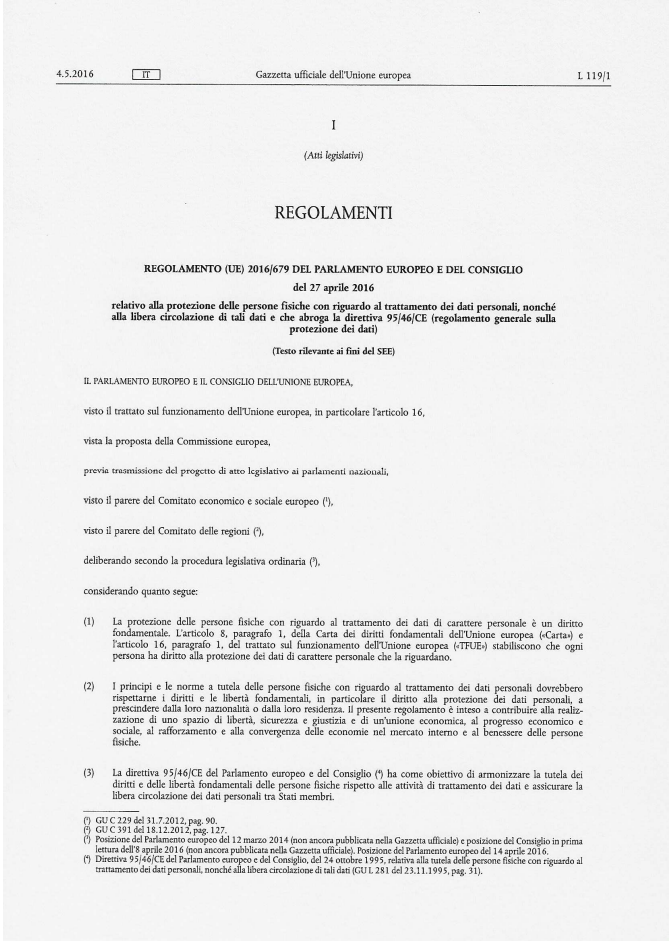
EVOLUZIONE NORMATIVA EUROPEA

Nel gennaio 2012 la Commissione europea ha presentato ufficialmente il cosiddetto "pacchetto protezione dati" con lo scopo di garantire un quadro coerente ed un sistema complessivamente armonizzato in materia nell'Ue.

Esso si compone di due diversi strumenti:

- **una proposta di Regolamento** concernente "la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati", volta a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico, e destinata a sostituire la Direttiva 95/46

- **una proposta di Direttiva** indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali, che sostituirà (ed integrerà) la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia (che l'Italia non ha, peraltro, ancora attuato).



4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/1

I

(Atti legislativi)

REGOLAMENTI

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)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo (1),

visto il parere del Comitato delle regioni (2),

deliberando secondo la procedura legislativa ordinaria (3),

considerando quanto segue:

(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

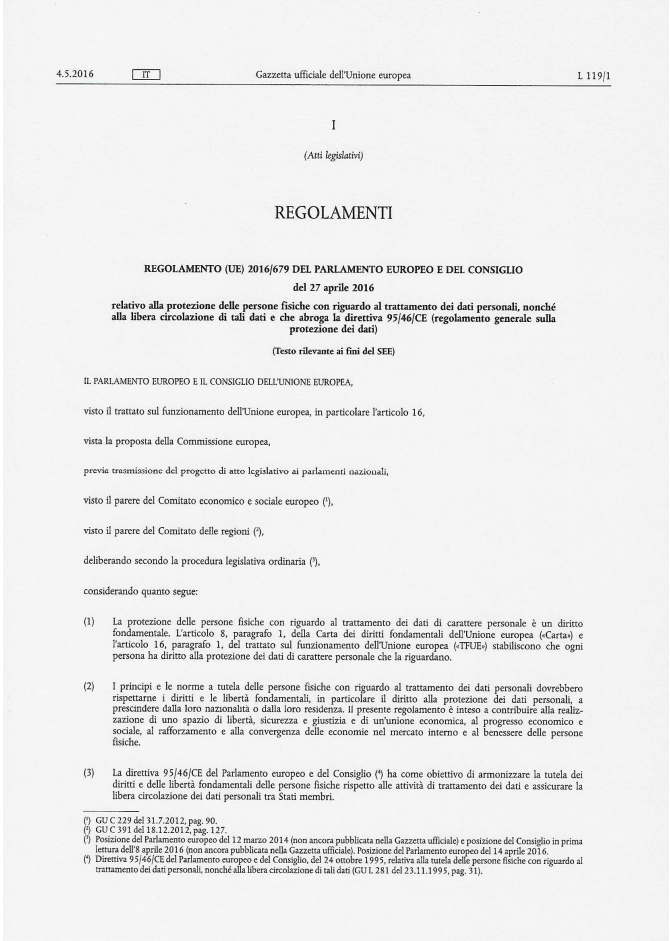
(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

(3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio (4) ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

(1) GU C 229 del 31.7.2012, pag. 90.
(2) GU C 391 del 18.12.2012, pag. 127.
(3) Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.
(4) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

… segue …

- **Il 4 maggio 2016**, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) 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 5 maggio 2016** è entrata ufficialmente in vigore la Direttiva, che dovrà essere recepita dagli Stati membri entro 2 anni (schema di D.lgs. che dovrebbe attuare in Italia la Direttiva 2016/680).
- **Il 24 maggio 2016** è entrato ufficialmente in vigore il Regolamento, che definitivamente **applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018**.



4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/1

I

(Atti legislativi)

REGOLAMENTI

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)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo (1),

visto il parere del Comitato delle regioni (2),

deliberando secondo la procedura legislativa ordinaria (3),

considerando quanto segue:

(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

(3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio (4) ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

(1) GU C 229 del 31.7.2012, pag. 90.
(2) GU C 391 del 18.12.2012, pag. 127.
(3) Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.
(4) Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

In definitiva:

Art. 99 - ENTRATA IN VIGORE E APPLICAZIONE:

Il presente regolamento **entra in vigore** il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea = **24 maggio 2016**

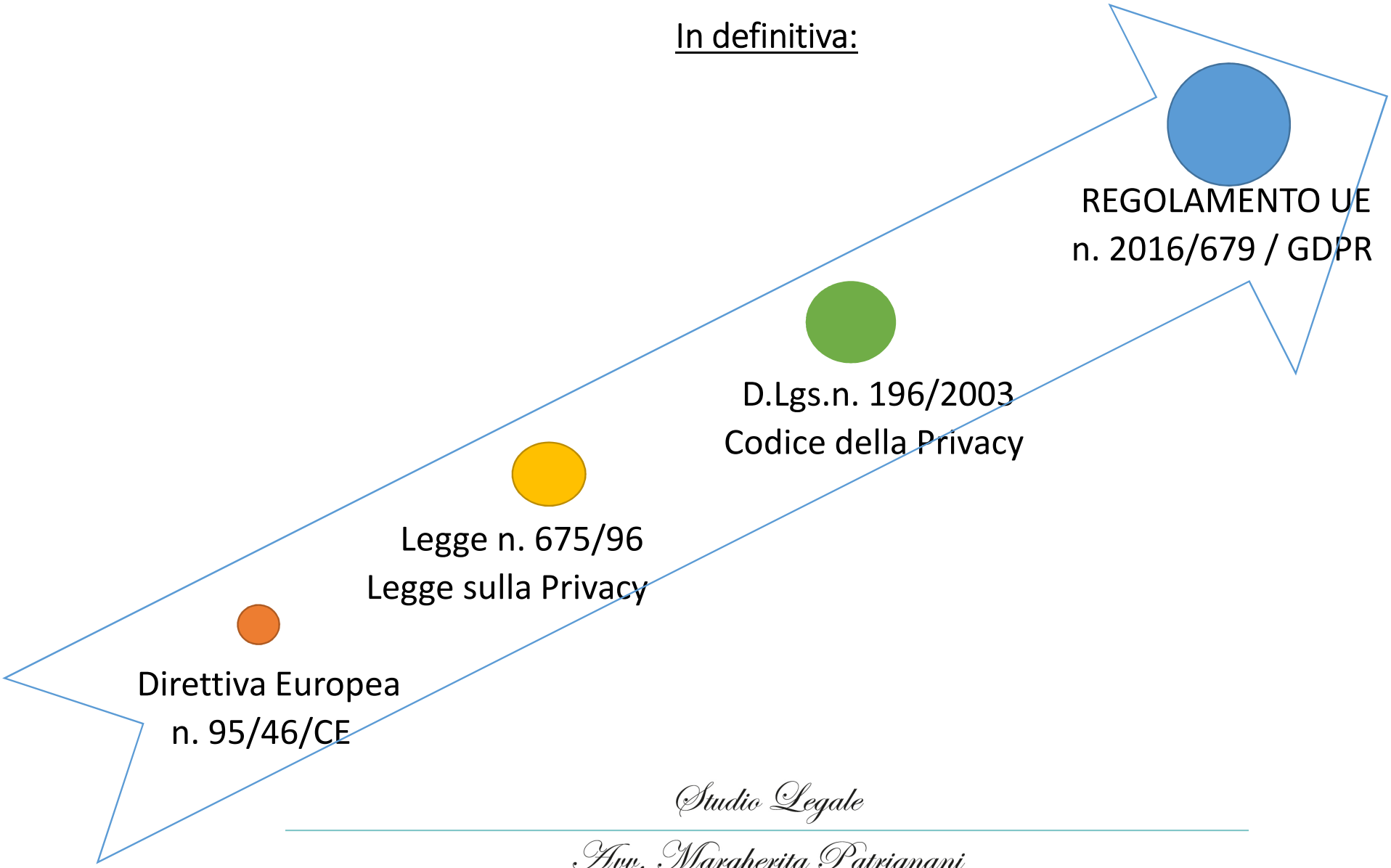
Esso **si applica** a decorrere **dal 25 maggio 2018**

Il presente regolamento è **obbligatorio** in tutti i suoi elementi e **direttamente applicabile** in ciascuno degli Stati membri.

La direttiva 95/46/CE è abrogata a decorrere dal 25 maggio 2018

=> fino ad allora si applicano le regole attuali

In definitiva:



Principi applicabili al trattamento – Art. 5

LICEITA'-CORRETTEZZA-TRASPARENZA

LIMITAZIONE DELLA FINALITÀ = dati raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità

MINIMIZZAZIONE DEI DATI = adeguati, pertinenti e limitati a quanto necessario

ESATTEZZA = esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti

LIMITAZIONE DELLA CONSERVAZIONE = conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità

INTEGRITÀ E RISERVATEZZA = trattati in modo 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

… segue …

RESPONSABILIZZAZIONE = ACCOUNTABILITY !!!

Il titolare del trattamento è competente per il rispetto dei principi e in grado di comprovarlo

LE NOVITA' DEL REGOLAMENTO

- Il nuovo principio di **responsabilizzazione (*accountability*)** è un punto centrale del Regolamento che dispone l'obbligo per il Titolare di mettere in atto "*misure tecniche e organizzative adeguate*" che devono essere costantemente monitorate ed aggiornate, se necessario, "**per garantire, ed essere in grado di dimostrare**" che il trattamento è effettuato conformemente al Regolamento.
- È obbligatorio proteggere i dati fin dalla progettazione **(Privacy by Design)** e per impostazione predefinita **(Privacy by Default)**.
- I diritti degli interessati sono ampliati e comprendono il nuovo **diritto alla portabilità dei dati ed il diritto all'oblio** (prima riconosciuto solo a livello giurisprudenziale), il diritto di essere informato con modalità trasparenti e con linguaggio semplice e chiaro, il diritto di accesso, il diritto di rettifica, la limitazione del trattamento, il diritto di opposizione, il diritto di non essere sottoposto ad un processo decisionale automatizzato, il diritto di essere informato della rettifica o cancellazione dei dati, il diritto al risarcimento del danno materiale o immateriale.
- In caso di trattamento effettuato **da un'Autorità pubblica o un organismo pubblico**, o se il Titolare o il Responsabile effettuano un trattamento che richiede un monitoraggio su larga scala, oppure se vengono effettuati trattamenti su larga scala di categorie particolari di dati o dati relativi a condanne penali o reati, è obbligatorio designare **il Responsabile della protezione dei dati (*Data Protection Officer*).**

… segue …

- È obbligatoria per il Titolare ed il Responsabile la tenuta di un **registro** **in forma scritta anche in formato elettronico delle attività di trattamento svolte**.
- **L'informativa** da rendere all'interessato deve essere concisa, trasparente, intellegibile e facilmente accessibile, deve essere resa con un linguaggio semplice e chiaro, anche in combinazione con icone standardizzate.
- Devono essere rispettare le condizioni per il rilascio di un valido consenso da parte di **minori**.
- Le **misure di sicurezza ed organizzative** adottate devono garantire un **livello di sicurezza adeguato** al rischio.
- Le **persone deputate al trattamento dei dati personali** (che corrisponderebbero agli attuali "incaricati") devono essere **autorizzate** espressamente ed istruite.
- Qualsiasi violazione di dati personali (***c.d. data breach***) deve essere **notificata al Garante** e, in presenza di determinati presupposti, anche **agli interessati** entro il termine di 72 ore. Viene invece eliminato l'obbligo di notificazione preventiva ex art. 37, D.Lgs. 196/2003.

… segue …

- L'approccio deve essere basato sul rischio ed è obbligatorio, nei casi previsti per legge, effettuare una **valutazione di impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment) e consultare preventivamente** l'autorità di controllo se la valutazione di impatto evidenzia un rischio elevato in assenza di misure per attenuare il rischio.
- L'adozione di **codici di condotta e di meccanismi di certificazione** possono essere di ausilio al Titolare e al Responsabile per dimostrare la conformità alle disposizioni del Regolamento.
- Sono attribuiti **maggiori poteri** alle **autorità di controllo nazionali**, definiti i compiti e poteri **dell'autorità di controllo capofila** in caso di trattamenti transfrontalieri, istituito il **Comitato Europeo per la protezione dei dati**.
- Le **sanzioni** sono particolarmente **severe** ed equivalenti in tutti gli Stati membri. Le sanzioni amministrative pecuniarie, che dovranno essere effettive, proporzionate e dissuasive, potranno arrivare **fino a euro 20 milioni**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore. Gli Stati membri hanno facoltà di stabilire, inoltre, norme relative ad altre sanzioni.

AMBITO DI APPLICAZIONE

- Il Regolamento **si applica:** a qualsiasi **TRATTAMENTO DI DATI PERSONALI** contenuti in un archivio o destinati a figurarvi, indipendentemente dal fatto che si tratti di un trattamento interamente o parzialmente automatizzato, ovvero non automatizzato

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*".

- Il Regolamento **si applica:**

- ai Titolari e Responsabili del trattamento **stabiliti in uno Stato dell'Unione Europea**, ovvero in un luogo soggetto al diritto di uno Stato membro, indipendentemente dal fatto che il trattamento sia effettuato nell'Unione;
- Inoltre, ai Titolari o Responsabili **non stabiliti nell'Unione Europea** se trattano i dati personali di interessati che si trovano nell'Unione Europea, quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi / il monitoraggio del loro comportamento .

… segue …

- Il Regolamento **non si applica:**

- al 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 (cfr. considerando 14);
- al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a **carattere esclusivamente personale o domestico** e quindi senza una connessione con un'attività commerciale o professionale (cfr. considerando 18*);
- a informazioni **anonime**, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato (cfr. considerando 26);
- ai dati personali delle persone **decedute -** Tuttavia, il Regolamento consente ai singoli Stati membri di prevedere norme riguardanti il trattamento di dati personali di persone decedute (cfr. considerando 27 - art. 9, comma 3, del D.Lgs. 196/2003).

DUNQUE, IL REGOLAMENTO SI APPLICA AL TRATTAMENTO DEI DATI PERSONALI **DELLE PERSONE FISICHE – AVENTI UNA CONNESSIONE CON UN'ATTIVITA' COMMERCIALE O PROFESSIONALE**

… segue: 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:**

raccolta

registrazione

organizzazione

strutturazione

conservazione

Adattamento / modifica

estrazione

consultazione

uso

Comunicazione mediante trasmissione

Diffusione / altra forma di messa a disposizione

Raffronto / interconnessione

limitazione

distruzione

cancellazione

… segue: DEFINIZIONI:

- **DATO PERSONALE = qualsiasi informazione** (nome, codice fiscale, immagine, voce, impronta digitale, traffico telefonico) **riguardante una persona fisica** (definita «interessato») **identificata o identificabile**
- **IDENTIFICABILE =** la persona fisica che può essere identificata, **direttamente o indirettamente**, anche mediante il riferimento ad ulteriori elementi ➡ Se l'identificazione richiede l'acquisizione di ulteriori dati per i quali occorrono tempi e costi irragionevoli, allora la persona non si può considerare identificabile

↓

Tale identificazione include anche **l'identificazione digitale** di un interessato, come ad esempio nel caso di utilizzo delle credenziali di autenticazione per usufruire di un servizio on line offerto dal titolare del trattamento

➡ Quindi il dato personale è un **concetto dinamico**, che va sempre riferito al contesto, nel senso che anche se un'informazione isolata non è in grado di portare all'identificazione di un individuo, il fatto che detta informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati ne determina la natura di dato personale.

… segue : DATI IDENTIFICATIVI - ESEMPI

- nome e cognome
- indirizzo di casa
- indirizzo email
- numero identificativo nazionale
- numero di passaporto
- indirizzo IP (quando collegato ad altri dati)
- login e password
- numero di targa del veicolo
- numero di patente
- volto, impronte digitali o calligrafia
- numeri di carta di credito
- identità digitale
- data di nascita
- luogo di nascita
- informazioni genetiche
- numero di telefono
- account name o nickname
- registrazione vocale

Altri esempi: login, cookie, dati di geolocalizzazione, voce, immagini, filmati, fotografie, numero di telefono, codice fiscale, impronta digitale, ore di servizio prestate da un dipendente, informazioni sul comportamento di un lavoratore, informazioni sulle condizioni patrimoniali

Dati pseudonimi sono quei dati personali nei quali gli elementi identificativi sono stati sostituiti da elementi diversi, quali stringhe di caratteri o numeri (hash), oppure sostituendo al nome un nickname, purché sia tale da rendere estremamente difficoltosa l'identificazione dell'interessato - a differenza di quelli anonimizzati, **sono comunque dati personali** (in quanto consentono l'identificazione della persona, anche se indirettamente, tramite incrocio con altre informazioni)

… segue: PARTICOLARI CATEGORIE DI DATI PERSONALI

ART. 9 «ex dati sensibili»

- i dati personali che rivelino **l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale**;
- i **dati genetici** (NOVITA'!) = caratteristiche genetiche ereditarie o acquisite che risultino dall'analisi di un campione biologico (DNA);
- i **dati biometrici** intesi a identificare in modo univoco una persona fisica, quali l'immagine facciale o i dati dattiloscopici - ad esempio negli aeroporti dove l'immagine dell'individuo viene scansionata per identificarlo (NOVITA');
- i dati relativi alla **salute** o alla **vita sessuale** o all'**orientamento sessuale** della persona.

ART. 10: dati relativi a condanne penali e reati

- Provvedimenti di cui al casellario giudiziario e all'anagrafe delle sanzioni amministrative dipendenti da reato (D.lgs.231/2001)
- Condanne penali e ai reati o a connesse misure di sicurezza
- La semplice qualità di imputato o indagato ai sensi del codice di procedura penale

… segue …

I DATI DEI MINORI: ART. 8

L’art. 8 del Regolamento dispone che, per quanto riguarda l'offerta diretta di servizi della società dell'informazione, **la validità del consenso dipende dall’età del minore**.

In particolare:

- se il minore ha almeno 16 anni il consenso dallo stesso prestato è valido e conseguentemente il trattamento è lecito;
- se il minore ha invece meno di 16 anni, il consenso deve essere prestato o autorizzato dal titolare della responsabilità genitoriale quale *conditio sine qua non* per la liceità del trattamento.

In tal caso, è onere del Titolare del trattamento verificare che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore tenuto conto delle tecnologie disponibili.

BASE GIURIDICA DEL TRATTAMENTO

ART. 6 – IL TRATTAMENTO È LECITO IN BASE A:

1) **CONSENSO:** Il consenso dell'interessato autorizza il trattamento dei dati. Il consenso deve essere specifico, cioè legato ad una finalità precisa → Se il trattamento è basato sul consenso il titolare del trattamento deve **fornire l'informativa** e garantire la portabilità dei dati:

COSA CAMBIA:

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

COSA CAMBIA:

- **il titolare 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); 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" (cfr. considerando 39 e 42)**

BASE GIURIDICA DEL TRATTAMENTO

ART. 6 – IL TRATTAMENTO È LECITO IN BASE A:

2) **ADEMPIMENTO DI OBBLIGHI CONTRATTUALI:** Il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Sostanzialmente è una forma speciale di consenso. → **Occorre l'informativa**, e deve essere garantita la portabilità dei dati

3) **OBBLIGHI DI LEGGE CUI È SOGGETTO IL TITOLARE DEL TRATTAMENTO:** Nel caso di trattamento dei dati necessario per l'adempimento di obblighi derivanti da legge, regolamento o normativa comunitaria (come il trattamento per l'attività giornalistica) non occorre consenso, non si deve garantire la portabilità dei dati, → ma **occorre fornire l'informativa**, nella quale va indicata la base giuridica del trattamento. In questo caso la finalità deve essere specificata per legge

4) **INTERESSI VITALI DELLA PERSONA INTERESSATA O DI TERZI:** Il trattamento è ammesso se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Ma si può utilizzare come base giuridica **solo se** nessuna delle altre condizioni di liceità può trovare applicazione; non occorre consenso, non si deve garantire la portabilità dei dati, ma → **occorre fornire l'informativa**, nella quale va indicata la base giuridica del trattamento.

BASE GIURIDICA DEL TRATTAMENTO

ART. 6 – IL TRATTAMENTO È LECITO IN BASE A:

5) **LEGITTIMO INTERESSE PREVALENTE DEL TITOLARE O DI TERZI CUI I DATI VENGONO COMUNICATI:** Quando il trattamento è necessario per il perseguimento dei legittimi interessi 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. Non occorre consenso, non si deve garantire la portabilità dei dati, ➡ ma **occorre fornire l'informativa**, nella quale va indicata la base giuridica del trattamento.

COSA CAMBIA:

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» introdotto dal nuovo pacchetto protezione dati.

COSA NON CAMBIA:

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

RACCOMANDAZIONI:

Il Regolamento offre alcuni criteri per il bilanciamento in questione (cfr. considerando 47* - ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento, ai fini di prevenzione delle frodi)

BASE GIURIDICA DEL TRATTAMENTO

ART. 6 – IL TRATTAMENTO È LECITO IN BASE A:

6) **INTERESSE PUBBLICO O ESERCIZIO DI PUBBLICI POTERI:** Il trattamento 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 (tramite legge statale o dell'Unione) non richiede consenso, né si deve garantire la portabilità dei dati, ➡ ma **occorre fornire l'informativa**, nella quale va indicata la base giuridica del trattamento. La finalità deve essere specificata per legge.

NB:
Nei casi di esenzione da consenso, ovviamente, l'informativa sulla privacy dovrà riportare non la dicitura "accetto l'informativa sulla privacy", bensì la più corretta "HO LETTO L'INFORMATIVA SULLA PRIVACY", al fine di evitare l'assunzione di responsabilità in base al GDPR.

L'INFORMATIVA ALL'INTERESSATO: ARTT. 12 – 13 – 14

Un'informativa non corretta vanifica qualsiasi consenso reso dall'interessato e rende illecito il trattamento

QUANDO È DOVUTA:

- Se un sito web non permette alcuna registrazione degli utenti, e non tratta dati degli utenti, non occorre l'informativa privacy.
- L'informativa è sempre dovuta ogni qual volta vi sia una **raccolta e trattamento** dei dati (es. indirizzi IP, mail) degli utenti (es. compilazione moduli), per cui anche nel caso in cui il sito utilizzi cookie tramite i quali raccoglie dati degli utenti; è, altresì, dovuta **quando il consenso dell'interessato non è richiesto**, oppure quando l'interessato è tenuto obbligatoriamente **per legge** a fornire i dati.
- Se il sito permette la registrazione degli utenti, ma i dati vengono usati solo per fini del sito medesimo (es. mailing list) e non per l'invio di proposte commerciali etc., occorre solo l'informativa privacy (da linkare al modulo di registrazione per consentirne la consultazione), ma non occorre la raccolta del consenso.
- Invece, se il sito permette la registrazione degli utenti e raccoglie dati anche a fini promozionali e pubblicitari, compreso la trasmissione a terzi, occorre l'informativa privacy e il consenso deve essere espresso con accettazione separata dell'informativa.

… segue …

CONTENUTO MINIMO (artt. 13 e 14 – più ampio rispetto al passato):

- **dati identificativi** (nome, denominazione o ragione sociale, domicilio o sede) del titolare/responsabile del trattamento e, se designato, **i dati di contatto** del responsabile per la protezione dei dati (DPO), quindi un recapito al quale gli interessati potranno rivolgersi per esercitare i propri diritti;

- **finalità e modalità del trattamento** (non come vengono trattati i dati ma a quale fine, per quanto tempo sono trattati, se i dati verranno trasferiti all'estero e, in questo caso, attraverso quali strumenti);

- quale è la **base giuridica** del trattamento, quindi se si tratta di trattamento basato su consenso o giustificato da leggi, legittimi interessi (in questo caso specificando quale è il legittimo interesse), etc.;

- **natura obbligatoria o facoltativa** del conferimento dei dati e le conseguenze della mancata comunicazione dei dati, specificando che è possibile rifiutare il consenso a singoli trattamenti quali quelli a fini di marketing diretto;

- soggetti e categorie di soggetti ai quali i dati possono essere comunicati -«**destinatari**» - e l'ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica);

- **i diritti dell'interessato** (diritto di chiedere se dati personali sono presenti nella banca dati, diritto di prenderne visione e di chiederne la modifica, cancellazione, diritto di presentare reclamo all'autorità di controllo, eventuale diritto alla portabilità, diritto di revoca del consenso in qualsiasi momento);

- se il trattamento comporta **processi decisionali automatizzati** (come la profilazione) deve essere specificato indicando anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

All'interno dell'informativa privacy devono essere indicati anche i cookie che veicolano il sito, le modalità di disabilitazione dei cookie e, nel caso di cookie di terze parti, il link alle pagine delle privacy policy dei servizi delle terze parti (oltre al consenso per i cookie «di profilazione»)

Studio Legale

Avv. Margherita Patrignani

Si fa presente che l'informativa cookie è una sezione dell'informativa privacy, non un documento separato, per cui generalmente si ammette che possa essere una pagina diversa da quella che contiene l'informativa privacy, ma quest'ultima deve assolutamente richiamarla (link).

… segue …

TEMPI DELL'INFORMATIVA:

- L'informativa deve essere fornita all'interessato **prima di effettuare la raccolta** dei dati (se raccolti direttamente presso l'interessato)
- Nel caso di dati personali **non raccolti direttamente presso l'interessato** (es. dati da archivi pubblici, rese dai familiari dell'interessato…), 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).

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

… segue …

SANZIONI:

Una violazione in materia di informazione agli utenti può avere come conseguenza l'indagine da parte dell'autorità per la protezione dei dati, il quale può imporre sanzioni fino a 20 milioni di euro ed eventualmente anche il blocco di tutti i dati raccolti ed elaborati in violazione delle norme.

Inoltre, gli utenti acquistano il diritto di avviare una azione civile per il risarcimento dei danno contro il titolare del trattamento o comunque il gestore del sito.

… segue …

DIRITTI DELL'INTERESSATO:

- **Diritto di accesso =** diritto di ricevere una copia dei dati personali oggetto di trattamento – NOVITA': Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi - i titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali
- **Diritto di cancellazione (diritto all'oblio)** = diritto alla cancellazione dei propri dati personali in forma rafforzata (l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento) - obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione"

… segue …

DIRITTI DELL'INTERESSATO:

- **Diritto di limitazione del trattamento =** è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione bensì anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento – N.B. Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori
- **Diritto alla portabilità dei dati** NOVITA' = consente agli interessati di ricevere, dal titolare del trattamento, "i dati personali che lo riguardano forniti ad un titolare del trattamento" in modo che possa trasmetterli ad un altro titolare del trattamento (ad esempio, un'altra azienda). Il diritto alla portabilità dei dati è previsto, quindi, al fine di garantire il trasferimento dei propri dati da un servizio online ad un altro - **Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei)** - **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** - solo i dati che siano stati "forniti" dall'interessato al titolare

I SOGGETTI : INTERESSATO AL TRATTAMENTO

L'interessato (data subject) al trattamento è la persona fisica a cui si riferiscono i dati personali, o più esattamente il proprietario dei suoi dati

- I **DIRITTI** esercitabili sono:

esercitare l'opposizione al trattamento in tutto o in parte; - ottenere la cancellazione dei dati in possesso del titolare; - ottenere l'aggiornamento o la rettifica dei dati conferiti; - chiedere ed ottenere in forma intellegibile i dati in possesso del titolare (diritto di accesso); - chiedere ed ottenere trasformazione in forma anonima dei dati; - chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento.

- **ESERCIZIO** dei diritti: L'interessato può rivolgersi direttamente al titolare - Il termine per la risposta è data senza ingiustificato ritardo e al più tardi entro 1 mese per tutti i diritti. Tale termine può essere esteso a 3 mesi in casi di particolare complessità - L'esercizio dei diritti è in linea di massima **gratuito**

I SOGGETTI : TITOLARE DEL TRATTAMENTO

La persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza (data controller)

- l titolare del trattamento non è, quindi, chi gestisce i dati, ma chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali
- Nel settore privato il titolare del trattamento può essere una persona fisica oppure una persona giuridica. Nel settore pubblico in genere il titolare del trattamento è l'autorità, cioè una persona giuridica

il titolare è l'ente nel suo complesso (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc.) anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.) - In molti casi, tali soggetti potrebbero assumere, semmai, la qualifica di "responsabile"

I SOGGETTI : CONTITOLARE DEL TRATTAMENTO

Contitolarità (ART. 26):

E' possibile che coesistano più titolari del trattamento (contitolari o jointes controllers) che decidono congiuntamente di trattare i dati per una finalità comune. In tale caso la normativa impone ai contitolari di definire specificamente (con un atto giuridicamente valido) il rispettivo ambito di responsabilità e i compiti. In ogni caso, però, gli interessati possono rivolgersi indifferentemente ad uno qualsiasi dei contitolari.

Contenuto minimo dell'accordo interno:

- deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati;
- deve indicare le responsabilità dei contitolari con riferimento all'esercizio dei diritti dell'interessato e all'obbligo di informativa all'interessato;
- può designare un punto di contatto per gli interessati

I SOGGETTI : RESPONSABILE DEL TRATTAMENTO – ART. 28

Il responsabile del trattamento (data processor) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento

Responsabile interno od esterno?

- PER L'UE: Il ruolo del responsabile del trattamento di cui al regolamento europeo è chiaramente riservato ad un **soggetto esterno all'azienda**, con riferimento ai fornitori di servizi. Infatti, vi è uno specifico obbligo di predisporre un contratto per la designazione delle responsabilità a carico del responsabile.

In particolare il WP29 ricorda che il titolare del trattamento può decidere di trattare i dati all'interno della propria azienda oppure delegare in tutto o in parte le attività di trattamento dati ad un soggetto esterno. Quindi per agire come responsabile del trattamento occorre essere una persona fisica o giuridica distinta dal titolare e elaborare dati per conto di questi.

… segue …

Contratto di designazione

- Il titolare del trattamento può scegliere se avvalersi o meno **dell'esternalizzazione del servizio di trattamento** dei dati, ma una volta optato per tale soluzione non può fare a meno di nominare il soggetto in questione quale responsabile del trattamento
- **NOMINATO DAL TITOLARE -** la nomina deve avvenire tramite contratto o altro «*atto giuridico a norma del diritto dell'Unione o degli Stati membri*»
- il titolare delega al responsabile la concreta gestione del trattamento, affidandogli uno o più compiti specifici oppure una serie di compiti dettagliati in generale - Il responsabile a sua volta può nominare responsabili di secondo livello (SUB-RESPONSABILI) = il responsabile tratta i dati SOLO SU ISTRUZIONE DETTAGLIATA del titolare

… segue …

Obblighi:

- **OBBLIGHI DI TRASPARENZA:** Il responsabile riceverà, tramite l'atto giuridico (cioè per iscritto), tutte le istruzioni in merito ai trattamenti operati per conto del titolare, alle quali dovrà attenersi - Inoltre il responsabile del trattamento dovrà mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi che gli impone l'articolo 28 del Regolamento e dovrà tenere il registro dei trattamenti svolti
- **GARANTIRE LA SICUREZZA DEI DATI**: Egli deve adottare tutte le misure di sicurezza adeguate al rischio (art. 32 regolamento), tra le quali anche le misure di attuazione dei principi di privacy by design e by default, dovrà garantire la riservatezza, vincolando i dipendenti, dovrà informare il titolare delle violazioni avvenute, e dovrà occuparsi della cancellazione dei dati alla fine del trattamento
- **ATTUARE LE MISURE TECNICHE ED ORGANIZZATIVE** idonee a ridurre i rischi del trattamento
- **OBBLIGO DI AVVISARE, ASSISTERE E CONSIGLIARE IL TITOLARE:** Dovrà, quindi, consentire e contribuire alle attività di revisione, comprese le ispezioni (o audit)

I SOGGETTI : ATORIZZATO/INCARICATO DEL TRATTAMENTO – ART. 29

L'incaricato del trattamento è la persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di trattamento dei dati

↓

Il regolamento europeo non prevede espressamente la figura dell'incaricato (art. 30 D.lgs. 196/03), ma non ne esclude la nomina, facendo riferimento a «***persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile***» (art. 4)

- L'incaricato è, in sintesi, colui che effettua materialmente le operazioni di trattamento sui dati personali. Può essere solo una persona fisica, e deve agire sotto la diretta autorità del titolare del trattamento
- La normativa non prevede requisiti quantitativi, per cui anche la semplice presa visione di un dato personale (es. il magazziniere che consulta la bolla di consegna, il portantino che trasporta il malato e la cartella sanitaria) si qualifica come trattamento, e quindi necessita di un formale incarico perché non sia considerato illecito

… segue …

L’incaricato deve essere:

1. **autorizzato al trattamento da parte del Titolare o del Responsabile;**
2. **istruito adeguatamente**

ATTO DI AUTORIZZAZIONE/DESIGNAZIONE: La nomina dell'incaricato o degli incaricati (può avvenire anche con unico atto per più incaricati) deve avvenire con **forma scritta**, tramite atto nel quale sono indicati i nominativi e i compiti, compreso gli obblighi inerenti le misure di sicurezza. L'incaricato deve, ovviamente, attenersi strettamente alle istruzioni ricevute. La designazione non necessita di firma degli incaricati per accettazione, anche se è utile una presa visione quale prova della conoscenza dell'incarico.

E’ in linea con il principio di accountability

I SOGGETTI : RESPONSABILE PROTEZIONE DATI – ART. 37/39

Il Data Protection Officer (DPO), o anche Responsabile per la Protezione dei Dati (RPD), è una figura introdotta dal nuovo regolamento europeo

↓

Il DPO è un consulente esperto, che va ad affiancare il titolare nella gestione delle problematiche del trattamento dei dati personali

↓

Il ruolo di DPO può essere affidato ad uno dei dipendenti dell'azienda tramite atto di designazione – DPO INTERNO - ma può anche essere esternalizzato – DPO ESTERNO - a un fornitore di servizi (libero professionista o azienda / persona fisica o giuridica) tramite apposito contratto di servizi

Il DPO deve adempiere alle proprie funzioni in piena **autonomia ed indipendenza**, e **in assenza di conflitti di interesse**. In tal senso non può ricoprire tale incarico un soggetto che si trova ai vertici aziendali, quindi in grado di influenzare le scelte adottate in materia di trattamento dei dati.

… segue …

NOMINA :

- Effettuata (art. 37) **dal Titolare o dal Responsabile** del trattamento, in base ad un contratto – nominativo e dati di contatto vanno pubblicati e comunicati all'autorità Garante
- **Obbligatoria** solo in tre casi:

1. **Per le amministrazioni e gli enti pubblici [autorità pubblica/organismo pubblico]** (eccetto le autorità giudiziarie nell'esercizio delle loro funzioni) *GRUPPO ART. 29
2. **Se l'attività principale*** svolta dal titolare o dal responsabile del trattamento consiste nel trattamento di dati che per la loro natura, oggetto o finalità, richiedono il **controllo* regolare e sistematico degli interessati su larga scala*** GRUPPO ART. 29 - FAQ
3. Se l'attività principale consiste nel **trattamento su larga scala di dati sensibili, relativi alla salute, alla vita sessuale, genetici, giudiziari e biometrici**.

… segue …

LARGA SCALA :

Occorre tenere in considerazione alcuni elementi:

- il numero degli interessati coinvolti (in termini assoluti o in percentuale rispetto alla popolazione di riferimento);
- la quantità dei dati trattati;
- le diverse tipologie di dati trattati;
- la durata del trattamento;
- la portata geografica del trattamento.

*In tal senso sono trattamenti su larga scala quello dei **dati di viaggio** dei soggetti che usano un sistema di trasporto pubblico (es. il monitoraggio tramite carte di viaggio), il trattamento dei **dati dei pazienti** da parte di un ospedale, il trattamento di **dati di geolocalizzazione** della clientela per fini statistici, il trattamento dei **dati dei clienti di una banca o un'assicurazione**, il trattamenti dei dati personali per la **pubblicità comportamentale** (tramite cookie di profilazione), il trattamento di dati dei fornitori di **servizi telefonici o internet**. **Non sono trattamenti su larga scala quelli del singolo medico o del singolo avvocato**.

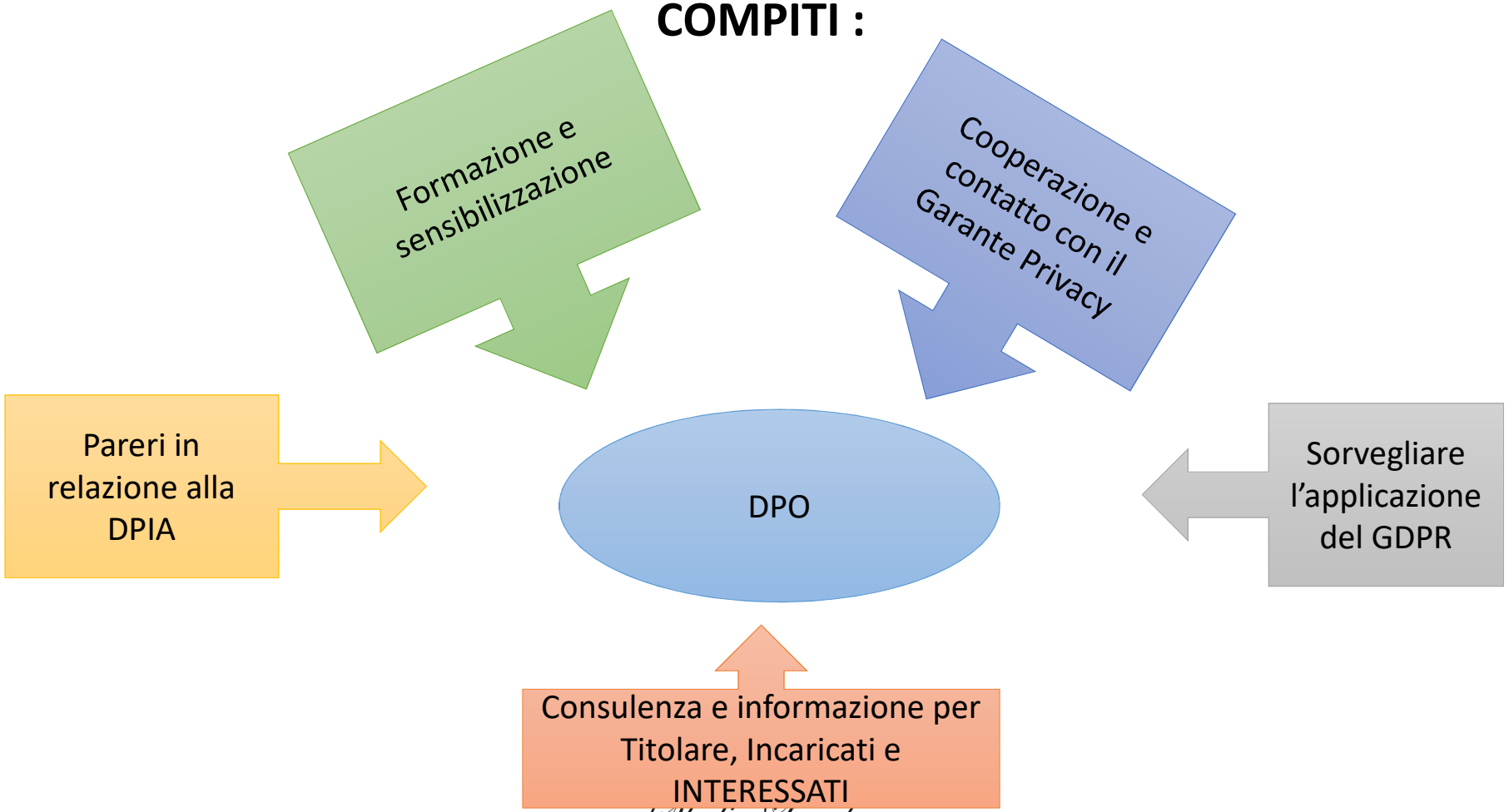
… segue …

A titolo esemplificativo :

- SOGGETTI OBBLIGATI: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; 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
- SOGGETTI NON OBBLIGATI: liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti 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

… segue …

COMPITI :



… segue …

RESPONSABILITA' :

Il DPO non è personalmente responsabile dell'inosservanza degli obblighi in materia di protezione dei dati personali, infatti è compito del titolare (art. 24) mettere in atto le misure tecniche ed organizzative adeguate.

Il DPO **risponde solo per lo svolgimento dei suoi obblighi di consulenza ed assistenza** nei confronti del titolare, che è (eventualmente in solido col responsabile) l'unico soggetto responsabile del rispetto della normativa. Il titolare, quindi, potrà solo avanzare pretese risarcitorie basate sulla **responsabilità contrattuale**, nei confronti del DPO.

Per prassi: che il DPO abbia il compito di realizzare l'inventario dei trattamenti e tenere il registro degli stessi. Questo nonostante sia il titolare, o il responsabile, ad essere obbligati a tale adempimento e responsabilità nei confronti degli interessati e delle autorità di controllo.

ARTICOLO 24 PARAGRAFO 1

«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, il titolare del trattamento 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»

ADOZIONE DI MISURE DI COMPLIANCE (check list, registro, valutazione di impatto, codice di condotta)

↓

IN RELAZIONE AL PRINCIPIO DI ACCOUNTABILITY

PRINCIPI FONDAMENTALI E MISURE DI ACCOUNTABILITY

➢ PRIVACY BY DESIGN E BY DEFAULT – ART. 25 [principio]

= LA PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE (PRIVACY BY DESIGN) E LA PROTEZIONE PER IMPOSTAZIONE PREDEFINITA (PRIVACY BY DEFAULT) QUALE OBBLIGO DEL TITOLARE

➢ **PRIVACY BY DESIGN:** mettere in atto misure tecniche ed organizzative adeguate a proteggere i dati sin da subito - privacy incorporata nel progetto (ad esempio, l'utilizzo di tecniche di **pseudonimizzazione o minimizzazione dei dati** – v. doc. identità)

↓

L'obbligo di privacy by design è basato sulla **valutazione del rischio**, che andrà fatta al momento della progettazione del sistema, quindi prima che il trattamento inizi, tenendo conto del tipo di dati trattati e dello stato della tecnologia, della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti (cfr. considerando 75/76)

PREVENIRE, NON CORREGGERE: CIOE' O PROBLEMI VANNO VALUTATI NELLA FASE DI PROGETTAZIONE

… segue …

- **PRIVACY BY DEFAULT:** per impostazione predefinita le imprese 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 di dati garantendo la non eccessività dei dati raccolti - privacy come impostazione di default (ad esempio, non deve essere obbligatorio compilare un campo di un form il cui conferimento di dati è facoltativo)

↓

L'introduzione di tali due principi obbliga le imprese a predisporre una **valutazione di impatto privacy / UN SISTEMA DI GESTIONE DEL RISCHIO** ogni volta che avviano un progetto che prevede un trattamento di dati.

NOMINA DPO/RPD + DPIA + REGISTRO + NOTIFICA DELLE VIOLAZIONI QUALI MISURE DI ACCOUNTABILITY

… segue …

PRIVACY BY DEFAULT: Questo implica che il titolare dei dati personali che vengono raccolti in occasione di registrazioni a servizi telematici o della stipula di contratti, o in breve in ogni caso in cui ciascuno di noi rende i propri dati ad un terzo, devono essere trattati sempre attraverso un **percorso di politica aziendale o amministrativa interna che ne tuteli la diffusione**.

- Intanto, ne deriva che le tutte le valutazioni che il titolare del trattamento deve effettuare in tema di protezione dei dati personali devono essere compiute **a monte**, cioè prima di procedere al trattamento dei dati vero e proprio
- il titolare deve svolgere un'analisi preventiva della situazione complessiva e adottare un approccio pratico che si dovrà, a sua volta, concretizzare in una serie di attività specifiche e dimostrabili
- Le soluzioni a cui il titolare del trattamento potrà affidarsi potranno consistere, ad esempio, nella riduzione al minimo del trattamento dei dati personali, nella pseudonimizzazione dei dati personali, nella massima trasparenza sulle finalità e sulle modalità del trattamento di dati personali, nel consentire all'interessato di controllarne il trattamento rendendo facilmente ed effettivamente esercitabili i diritti previsti dal Regolamento.

… segue …

VALUTAZIONE DEL RISCHIO :

PROBABILITA’ + IMPATTO = GRAVITA’ DEL RISCHIO

*** * ***

GESTIONE DEL RISCHIO:

ANALISI DEL CONTESTO + VALUTAZIONE DEL RISCHIO + TRATTAMENTO DEL RISCHIO = SISTEMA DI GESTIONE DEL RISCHIO

PRINCIPI FONDAMENTALI E MISURE DI ACCOUNTABILITY

➢ SICUREZZA DEL TRATTAMENTO – ART. 32 [principio]

= obbligo generale in capo al Titolare ed al Responsabile di adozione di misure tecniche ed organizzative "adeguate" al rischio

↓

in particolare dei rischi che derivano 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

… segue …

Le misure di sicurezza **comprendono**, fra l'altro:

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;

d) una **procedura per testare, verificare e valutare regolarmente l'efficacia** delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

e) l'**istruzione delle persone autorizzate** al trattamento dal Titolare e dal Responsabile

IL REGISTRO DEI TRATTAMENTI – ART. 30 [misura]

ONERE DI TENUTA del registro è a carico del **titolare** e, se nominato, del **responsabile** del trattamento

La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e ad una corretta pianificazione dei trattamenti

Il registro deve essere tenuto in **forma scritta, anche in formato elettronico**, e va esibito all'autorità di controllo (Garante) in caso di verifiche

ESENZIONE dall'obbligo di tenuta del registro per le imprese o le organizzazioni con **meno di 250 dipendenti**, a meno che il trattamento effettuato:

- possa presentare un rischio per i diritti e le libertà degli interessati
- non sia occasionale
- o includa il trattamento di categorie particolari di dati, cioè dati sensibili o giudiziari

… segue …

CONTENUTO MINIMO:

A. **nome e i dati di contatto** del titolare del trattamento e, se nominati, 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 cui al secondo comma dell'articolo 49, 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** di cui all'articolo 32, paragrafo 1.

Il registro sostituisce la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare) – controllo ex post

L'autorità di controllo belga ha predisposto un modello non ufficiale del registro, poi tradotto in inglese

DPIA (Data Protection Impact Assessment) – ART. 35 [misura]

E’ un’analisi da effettuare **PRIMA di procedere al trattamento** dati al fine di **VALUTARE I RISCHI** per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, così da identificare le misure necessarie per la mitigazione di tali rischi

↓

Si tratta di uno dei criteri previsti dal regolamento generale per la progettazione dei trattamenti, che appunto prevede **l'obbligo di una analisi del rischio del trattamento**, e quindi della valutazione delle misure tecniche od organizzative che il titolare ritiene di dover adottare per ridurre l'eventuale rischio

Nonché per dimostrare che il trattamento dei dati personali rispetta il regolamento = **COMPLIANCE** (cfr. CONSIDERANDO 84)

… segue …

Chi svolge la valutazione?

La valutazione di impatto del trattamento **è un onere posto direttamente a carico del titolare del trattamento**

↓

Il titolare **deve consultarsi col DPO** (art. 35) quando svolge la valutazione di impatto, il quale DPO ha il compito di fornire, se richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento. Nel caso in cui il titolare non concordi con le indicazioni del DPO, dovrà motivare e documentare il suo dissenso

… segue …

Quando è obbligatoria la DPIA?

Quando un trattamento "possa presentare **un rischio elevato** per i diritti e le libertà delle persone fisiche" [cfr. Linee Guida* sui criteri] – maggiore è il numero di criteri soddisfatti, più è probabile che il rischio sia elevato

↓

- In particolare in caso di:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, compresa la profilazione;

b) trattamento su larga scala di dati sensibili o giudiziari (n. soggetti, volume dati, durata, portata geografica);

c) sorveglianza sistematica su larga scala di zone di accesso pubblico (piazza,

Le Autorità di controllo hanno un ruolo importante, in quanto possono stabilire, con un elenco pubblico, quali tipologie di trattamenti richiedono comunque la valutazione di impatto. Allo stesso modo, possono redigere un elenco delle tipologie di trattamenti per i quali la valutazione non è necessaria.

… segue …

Contenuto minimo delle DPIA?

Descrizione dei trattamenti previsti e delle finalità di tali trattamenti, compreso l'interesse legittimo perseguito dal titolare

Valutazione della necessità e proporzionalità dei trattamenti

Valutazione dei rischi per i diritti e le libertà degli interessati

Misure previste per mitigare i rischi e dimostrare la conformità al GDPR

Il CNIL (autorità di controllo francese) ha messo a disposizione un software open source per la valutazione di impatto sia nella versione standalone (da scaricare sul computer) che in quella online. Anche il Garante italiano segnala questo software come tool per realizzare la valutazione (**http://www.garanteprivacy.it/regolamentoue/DPIA#STRUMENTI**)

… segue …

Qual è lo scopo delle DPIA?

E’ un importante strumento per il Titolare, per **RAGGIUNGERE E DIMOSTRARE LA COMPLIANCE** al GDPR, in quanto rileva i rischi nel trattamento effettuato e descrive le misure di sicurezza adottate per ridurli

Sostiene il principio di *accountability* (responsabilizzazione) del Regolamento UE 2016/679 (art. 5 comma 2) in funzione della COMPLIANCE (conformità giuridica)

E’ il titolare a decidere se un dato trattamento sia tale da non «presentare un rischio elevato»: in tali casi **il titolare deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d’impatto**, nonché includere/registrare i punti di vista del RPD

… segue …

SANZIONI:

- Per mancata esecuzione di una DPIA
- Per esecuzione errata di una DPIA
- Per mancata consultazione dell'autorità di controllo

SANZIONE AMMINISTRATIVA PECUNIARIA FINO A 10 MILIONI DI EURO OPPURE, NEL CASO DI UNA IMPRESA, FINO AL 2% DEL FATTURATO GLOBALE DELL'ANNO PRECEDENTE, A SECONDA DI QUALE DEI DUE IMPORTI SIA QUELLO SUPERIORE

NOTIFICA DELLA VIOLAZIONI DI DATI PERSONALI (DATA BREACH) – ART. 33/34 [misura]

= obbligo di notificare la violazione dei dati personali (c.d. "data breach") all'autorità di controllo e, in alcuni casi, anche agli interessati del trattamento

↓

DATA BREACH : si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni

↓

un data breach, quindi, non è solo un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali (furto di un notebook di un dipendente) - Il nuovo regolamento generale europeo prescrive specifici adempimenti nel caso di una violazione di dati personali

… segue … ITER

1. **<u>NOTIFICA</u> ALL'AUTORITA': IL TITOLARE NOTIFICA ALL'AUTORITA' DI CONTROLLO LA VIOLAZIONE** SENZA INGIUSTIFICATO RITARDO E, OVE POSSIBILE, **ENTRO 72 ORE** DAL MOMENTO IN CUI NE È VENUTO A CONOSCENZA

↓

solo se il titolare ritiene probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati

2. **<u>DOCUMENTAZIONE</u>**: IL TITOLARE È TENUTO A **DOCUMENTARE QUALSIASI VIOLAZIONE** DEI DATI PERSONALI (comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio) tramite un apposito registro delle violazioni, anche se non comunicate alle autorità
3. **<u>COMUNICAZIONE ALL'INTERESSATO</u>:** IL TITOLARE INFORMA SENZA RITARDO L'INTERESSATO

↓

Solo se ritiene che il <u>rischio</u> per i diritti e le libertà degli interessati è <u>elevato</u>

OBBLIGHI DEL TITOLARE E DEL RESPONSABILE:

A. NOMINA IL RPD/DPO

B. TENUTA DEL REGISTRO

C. DPIA (solo titolare)

D. NOTIFICA VIOLAZIONE (solo titolare)

- **PRIVACY BY DESIGN / BY DEFAULT: VALUTAZIONE DEL RISCHIO – A. + B. + C.**
- **MISURE DI SICUREZZA: TRATTAMENTO DEL RISCHIO – D.**

TUTELA DA TRATTAMENTO ILLECITO – ARTT. 77/82

- **IL RECLAMO ALL'AUTORITÀ DI CONTROLLO;**
- **IL RICORSO GIURISDIZIONALE;**
- **IL DIRITTO AL RISARCIMENTO DEL DANNO**

IN DEFINITIVA: PER NON RISCHIARE – 25 MAGGIO 2018

Identificazione dei principi di liceità e delle finalità del trattamento

↓

Analisi dei rischi in base alla probabilità e gravità

↓

Selezione solo di partner conformi alle norme privacy (Outsourcing)

↓

Adeguate misure di sicurezza dei dati, nei sistemi tecnologici e nei processi aziendali

↓

Nomina delle figure interne/esterne autorizzate al trattamento

↓

Compliance ai provvedimenti delle Autorità Garanti

APPLICAZIONI PRATICHE

Si segnalano per la loro rilevanza nell'organizzazione del lavoro quotidiano di studio alcuni esempi e casi di interesse in materia di privacy:

✓ ***Tenuta dei fascicoli relativi ai clienti***

Contrariamente a quanto ritenuto nella prassi professionale, **non occorre depennare, per motivi attinenti alla privacy, il nome dei clienti dalla copertina dei fascicoli cartacei**, **utilizzando numeri identificativi**. Resta invece necessario adottare opportune modalità per rendere i fascicoli e la relativa documentazione accessibile agli autorizzati al trattamento nei casi e per le finalità previsti (cfr. CONSIDERANDO 15: «*Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine*»)

… segue …

✓***<u>Cloud Computing e archiviazione – LINEE GUIDA GARANTE 24/05/2012</u>***

- Il titolare del trattamento deve assicurarsi che siano adottate misure tecniche e organizzative volte a ridurre al minimo i rischi
- E' fondamentale verificare in quale Stato sono conservati i dati caricati sulla "nuvola" – la normativa sulla privacy, al fine di tutelare le persone interessate, prevede che i dati possano essere "esportati" in Paesi fuori dall'Unione europea solo in precisi casi e quando sia offerta una protezione adeguata rispetto a quella prevista dalla legislazione comunitaria – NB: **il consenso dell'interessato esplicito** al trasferimento <u>deroga</u> alla mancanza di una decisione di adeguatezza e di garanzie adeguate

- PS: per DROPBOX certificazione PRIVACY SHIELD (Scudo per la Privacy EU-USA)

… segue …

✓***<u>Cloud Computing e archiviazione – LINEE GUIDA GARANTE 24/05/2012</u>***

E’ lecito il trasferimento di dati all’estero SE:

1. DECISIONE DI ADEGUATEZZA DELLA COMMISSIONE
2. GARANZIE ADEGUATE
3. CONSENSO ESPLICITO DELL’INTERESSATO

… segue …

✓***Periodo di conservazione***

Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il professionista dovrebbe **stabilire ex ante un termine per la cancellazione o per la verifica periodica** del rispetto del principio di limitazione (per es. criterio civilistico che individua in dieci anni il periodo di conservazione dei documenti)

In linea generale si suggerisce di evidenziare sempre nel contratto concluso con il cliente il periodo di conservazione e, in assenza di riferimenti normativi, **i criteri necessari** ai fini dell'individuazione del periodo di conservazione.

«I Suoi dati personali, oggetto di trattamento per le finalità sopra indicate, saranno conservati per il periodo di durata del contratto e, successivamente, per il tempo in cui il professionista sia soggetto a obblighi di conservazione per finalità fiscali o per altre finalità, previsti da norme di legge o regolamento [(p.to a) art. 13 Co. 2 GDPR]»

… segue …

✓***DPO/RPD***

Varrà evidenziare che il Garante non ritiene obbligatoria la nomina del DPO "*in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale*". Nondimeno, tale nomina "in ogni caso, resta comunque raccomandata, anche alla luce del principio di <<accountability>> che permea il Regolamento"25.

Si suggerisce in ogni caso di indicare per ciascuno studio professionale almeno un "**Referente GDPR**" al quale fare riferimento (c.d. "**punto di contatto**") sia ai fini di eventuali verifiche e controlli sia al fine di consentire un migliore e agevole esercizio dei diritti degli interessati (Cfr. Garante privacy, Nuove faq sul responsabile della protezione dei dati in ambito privato, documento web n. 8036793 del 26 marzo 2018; Linee Guida sui responsabili della protezione dei dati, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017)

… segue …

✓ ***Aspetti documentali***

Ai fini del corretto adempimento degli obblighi derivanti dal GDPR, **ogni misura adottata dovrà essere documentabile** in ossequio al principio di "responsabilizzazione". Pertanto, nonostante il registro dei trattamenti previsto dal GDPR non sia obbligatorio per gli studi professionali, se ne consiglia l'adozione.

✓ ***Informativa***

PS: Trattamento per finalità diverse da quelle per cui i dati sono stati raccolti:

Qualora il professionista, in qualità di titolare del trattamento, intenda trattare ulteriormente i dati personali per finalità diverse da quella per cui gli stessi sono stati raccolti, prima di tale ulteriore trattamento deve fornire all'interessato una nuova informativa relativa a tale diversa finalità e ogni ulteriore informazione pertinente. Tale informativa potrà costituire appendice al contratto già stipulato con il Cliente

… segue …

✓***Deleghe autorizzative***

Il titolare del trattamento dovrà autorizzare i propri collaboratori e tirocinanti ad effettuare il trattamento dei dati personali degli interessati

✓***Organizzazione di studio***

il titolare del trattamento (dominus di Studio o Associazione o Società Professionale) dovrà impostare tutte le proprie attività e l'organizzazione di studio rispettando i principi della "privacy by design" e "privacy by default", adottando conseguentemente, adeguate misure tecniche ed organizzative, prima che il trattamento dei dati personali abbia inizio, idonee a consentire il rispetto dei principi di minimizzazione dei dati, limitazione della conservazione e ad evitare la comunicazione dei dati a persone non autorizzate.

Inoltre, si consiglia di prevedere, sempre, una **procedura per i c.d. "data breaches"** (violazione dei dati personali) nonché appositi **meccanismi per consentire l'esercizio dei diritti** dell'interessato secondo le modalità descritte dal GDPR (es. diritto di accesso)

… segue …

E’ necessario impiegare meccanismi che permettano di evitare accessi abusivi ai dati, alterazioni o modifiche degli stessi, cancellazioni, divulgazioni non autorizzate o violazioni di altro tipo = **misure di sicurezza**:

- impiegando meccanismi antielusione come i **firewall**
- utilizzando (e facendo utilizzare) **password** sicure per accedere ai sistemi informatici dello studio in cui sono archiviati dati personali, provvedendo a redigere opportune **best practice** su come tali password dovranno essere custodite e amministrate e prevedendo, se si dispone di un sito web, con cui ad esempio è possibile inviare richieste mediante la compilazione di form, l’impiego di **protocolli SSL** (Secure Sockets Layer, livello di socket sicuri)
- Allo stesso modo con cui il sostituto o il collaboratore può accedere ai fascicoli cartacei dei pazienti, può certamente accedere ai dati sanitari memorizzati nel computer dello studio, però è necessario che vi acceda con un **proprio nome utente e una propria password**, in modo che sul computer rimanga una “traccia informatica” di chi, come e quando ha acceduto al sistema.

… segue …

- importante per il transito dei dati è l'uso di **chiavette USB dotate di password** o anche chiavette che consentono di criptare i dati ivi contenuti (il Regolamento, infatti all'articolo 32 consiglia proprio l'impiego di strumenti che consentano di cifrare i dati o comunque usare la pseudonimizzazione)
- strumenti che permettano di effettuare il **backup**, meglio se continuo dei dati, come ad esempio potrebbe essere un servizio di cloud fornito da un soggetto terzo di cui sarà necessario vagliare l'affidabilità e il grado di sicurezza offerto prima di sottoscrivere il contratto, designando, tra l'altro, anch'esso, responsabile del trattamento
- mantenere i **sistemi operativi sempre aggiornati** ed i vari programmi e le applicazioni utilizzate, determinando, a priori, una **manutenzione periodica**
- controllare i vari **devices, come smartphone o tablet**, impostando una limitazione all'uso dei dati contenuti, se su di essi sono conservati o transitano in qualche modo anche dati relativi a clienti

… segue …

- l'impiego di una **procedura per testare, verificare e valutare** regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento ex articolo 32, lettera d (cfr. esempio CHECK LIST)

N.B. Si tenga poi presente che anche il professionista, in qualità di titolare del trattamento (o contitolare, mentre il responsabile dovrà comunicare un'eventuale violazione al titolare) è chiamato a comunicare al Garante eventuali violazioni sui dati personali entro 72 ore dal momento in cui ne viene a conoscenza, pertanto, occorrerà pensare anche a **procedure preventive che consentano di intervenire velocemente sulla violazione e procedere tempestivamente alla comunicazione all'autorità**.

DUNQUE: I PUNTI ESSENZIALI

- SISTEMA DI AUTENTICAZIONE INFORMATICA: credenziali di autenticazione – password robusta e aggiornata -SISTEMA DI AUTORIZZAZIONE PER GLI INCARICATI

- AGGIORNAMENTO PERIODICO PROGRAMMI – RESTORE – BACK UP

- UTILIZZO DI SERVER, NAS E GRUPPI DI CONTINUITA'

- CORRETTA CUSTODIA DEI DOCUMENTI CARTACEI: sistemi di allarme, armadietti chiusi a chiave – SICUREZZA SISTEMA INFORMATICO: firewall, antivirus, password PC

- CONSERVAZIONE: per il tempo necessario al perseguimento della finalità per cui sono stati raccolti = fin tanto che dura il rapporto di cura - per i 10 anni successivi al termine di esso (V. CODICE CIVILE)

- CRITTOGRAFIA: dell'intero hard disk [VeraCrypt – Bitlocker] o di singole cartelle [Easy File Locker (Windows) - HiddenDIR (Windows) - 7-Zip (Windows) - VeraCrypt (Windows/macOS)] o di singoli file [Encrypto (Windows/Mac) - Drag'n'Crypt ULTRA (Windows) -ProtectFile (Windows) - Easy File Locker (Windows) - PixelCryptor (Windows) - iSteg (Mac)

DUNQUE: IN PRATICA

- occorre fare un "**ASSESSMENT**", una valutazione di quali sono i dati che si detiene, del perché li si detiene e se ci possono essere dei rischi particolari nel loro utilizzo o conservazione

- mettere in atto misure adeguate e rapportate al caso concreto

- se si ha solo l'anagrafica dei propri clienti, blindare lo studio può essere uno spreco di denaro, se si conservano ingenti dati personali, usare solo una password banale sul proprio server rischia di essere considerato poco adeguato

check list che ha lo scopo di aiutare i professionisti a fare una autoanalisi nel proprio studio + sistema di gestione dei rischi

- **CHECK UP INIZIALE**
- **INFORMATIVA**
- **REGISTRO TRATTAMENTI**
- **LETTERE DESIGNAZIONE**
- **VALUTAZIONE RISCHI**
- **TRATTAMENTO RISCHI – sicurezza informatica-procedure**

… segue …

Al 25 maggio è FONDAMENTALE

avere (almeno) INIZIATO

un cammino di adeguamento

e poterlo DIMOSTRARE

GRAZIE PER L'ATTENZIONE !

Via S. Allende, 99 interno 1 - 47841 Cattolica (RN)
Cell. 328.3123467 - Mail margherita.patrignani@gmail.com
PEC margherita.patrignani@ordineavvocatirimini.it
P. Iva 04 008 510 408

Studio Legale

Avv. Margherita Patrignani