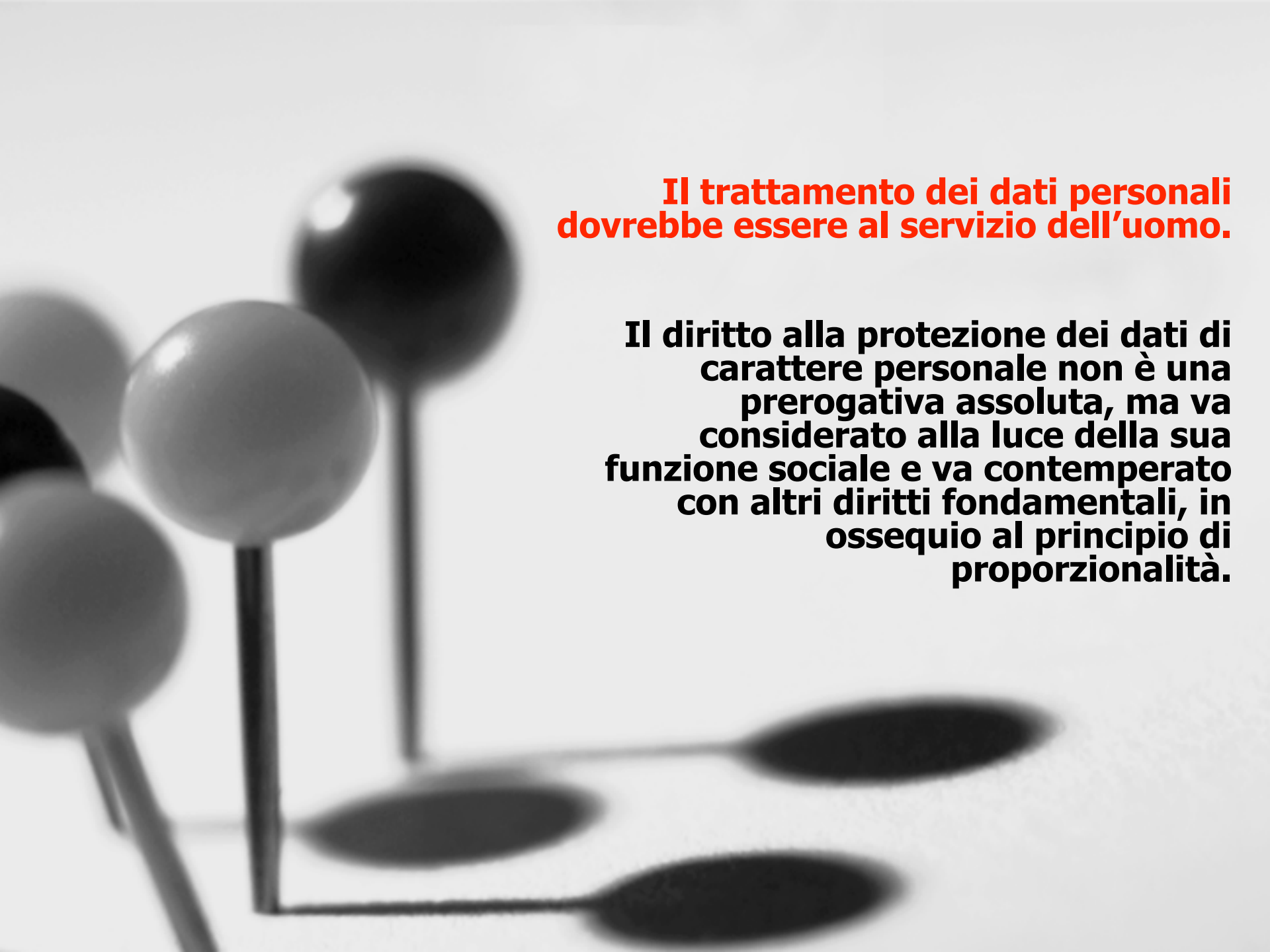
IL REGOLAMENTO UE 2016/679

avv. Matteo Grazioli

Arco, 25 maggio 2018

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 e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano
(considerato n. 1)



Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo.

Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica

(considerato n. 4)

Regolamento UE 2016/679

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 5 maggio 2016 è entrata ufficialmente in vigore la Direttiva, che dovrà essere recepita dagli Stati membri entro 2 anni.

Il 24 maggio 2016 è entrato in vigore il Regolamento, che diventerà definitivamente applicabile ed esplicherà i propri effetti in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Trattandosi di regolamento, non è soggetto a recepimento e quindi entrerà in vigore contemporaneamente all'interno dei 27 paesi membri dell'UE

Attualmente vi sono 27 differenti normative in materia di protezione dei dati personali

Principi e finalità del Regolamento

Il Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei loro dati personali.

Si fonda sul **principio di responsabilizzazione** (**accountability**) ed introduce nuove regole in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti (ad. es. accesso ed oblio), stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali.

Vengono privilegiati adempimenti "di tutela sostanziale" tramite nuove funzioni: valutazione dei rischi; principio di responsabilizzazione del titolare; valutazione di impatto; privacy by default; data protection officer; data breach.

Considerando:

1-7: principi e finalità
8- 10: facoltà per gli stati di integrare i contenuti del regolamento;
14- 15: applicabilità per persone fisiche;
18: esclusione per trattamento personale o domestico;
22: criterio dello "stabilimento";
26: dato personale, identificabilità e pseudonimizzazione;
27: non applicabilità per persone decedute;
32, 42, 43: requisiti del consenso;
34: dati genetici;
35: dati relativi alla salute;
38: minori;
39-40: liceità e correttezza;
50: principio di finalità della raccolta;
51-54: particolari categorie di dati;
58- 64: trasparenza e diritto di accesso;
65: diritto di oblio
66- 71: diritti dell'interessato;
72: profilazione;

74: responsabilità del titolare;
75- 85: indicazione dei rischi derivanti dal trattamento;
78-83: adeguatezza delle misure di sicurezza;
81: responsabile del trattamento;
82: registro del titolare;
85- 88: data breach;
89: notifica all'autorità di controllo;
90-95: valutazione di impatto;
97: DPO
98-99: adozione codici di condotta;
100: certificazioni;
101- 116: trasferimento extra UE;
117- 140: autorità di controllo;
141-145: tutele;
146: risarcimento danni;
149: riserva per gli stati di prevedere sanzioni penali;
154: pubblico accesso;
156: gestione archivi di interesse pubblico;
159-164: attività di ricerca.

Disposizioni generali

(artt. 1, 2, 3, 4)

oggetto e finalità: protezione delle persone fisiche con riferimento al trattamento dei loro dati personali - Art. 8 Carta Diritti Fondamentali UE)

nuovo ambito di applicazione materiale e territoriale

definizioni: dato personale (non è presente la definizione di "dato sensibile"); trattamento; pseudonimizzazione; archivio; titolare; responsabile; destinatario; terzo; violazione dati personali; autorità di controllo; ecc

Principi applicabili al trattamento di dati personali

(artt. 5, 6, 7)

liceità

correttezza e **trasparenza**

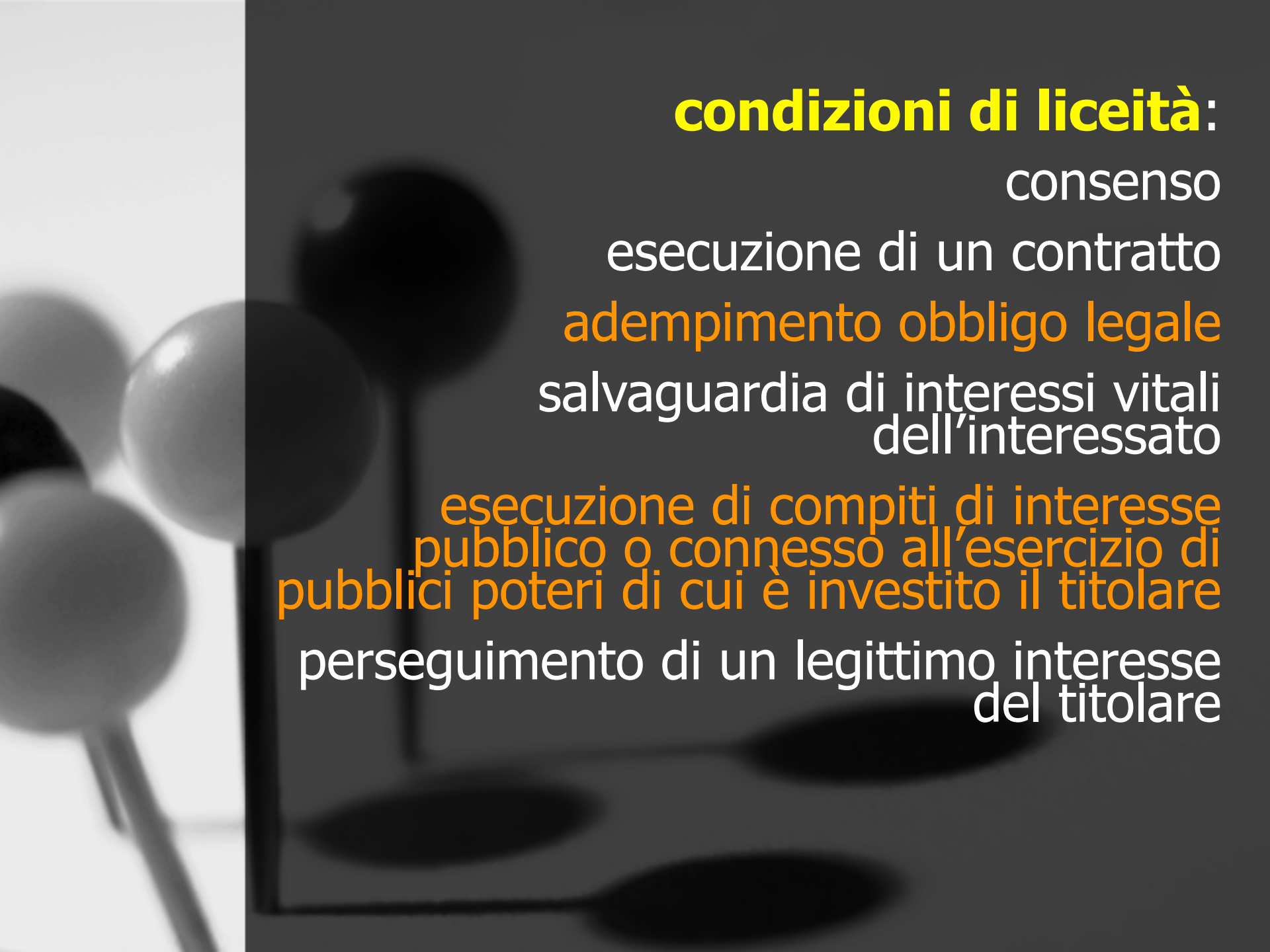
determinatezza dei fini della raccolta

temporalità del trattamento

adozione di misure tecniche e organizzative adeguate a garantire una adeguata sicurezza e protezione.

quando un trattamento è trasparente?

- quando sono esplicitati nelle informative i tempi di conservazione dei dati raccolti;
- quando nelle informative è indicato il diritto di proporre reclamo all'autorità di controllo e le coordinate di contatto di detta autorità;
- quando nelle informative viene segnalato il responsabile della protezione dei dati e le modalità per poterlo contattare;
- quando è rispettato l'obbligo di notificare una violazione dei dati all'autorità di controllo;
- quando è rispettato l'obbligo di comunicare una violazione dei dati agli interessati;
- quando viene segnalato il responsabile della protezione dei dati all'Autorità di controllo.



condizioni di liceità:

consenso

esecuzione di un contratto

adempimento obbligo legale

salvaguardia di interessi vitali dell'interessato

esecuzione di compiti di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare

perseguimento di un legittimo interesse del titolare

art. 9: trattamento di categorie particolari di dati personali

Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale è vietato.

Tale divieto non si applica se:

- è presente il consenso esplicito dell'interessato;

-il trattamento è necessario per assolvere ad obblighi ed esercitare diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, sicurezza e protezione sociale;

- il trattamento è necessario per tutelare un interesse vitale dell'interessato;

- il trattamento sia svolto da parte di una fondazione, associazione o enti no profit in relazione ai propri iscritti e i dati non siano diffusi o comunicati a terzi;

- il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;

- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

- il trattamento è necessario per motivi di interesse pubblico;

- il trattamento è necessario per finalità di medicina preventiva, medicina del lavoro, diagnosi, assistenza, terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitario o soclali;

- il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica;

- archiviazione nel pubblico interesse, ricerca scientifica o storica, fini statistici.

diritti degli interessati

Il Regolamento assegna all'interessato i seguenti diritti:

informativa (artt. 12-14): nuove modalità ("concisa, trasparente, intellegibile e facilmente accessibile") e nuovi contenuti rispetto all'art. 13 del d.lgs 196/03

diritto di accesso (art. 15)

rettifica (art. 16)

oblio (art. 17)

diritto ottenere la limitazione del trattamento (art. 18)

portabilità dei dati (art. 20)

opposizione al trattamento (art. 21)

PRIVACY "BY DESIGN"
E PRIVACY "BY DEFAULT"

privacy by design

principio di necessità art. 3 d.lgs 196/03: protezione dei dati fin dalla progettazione. Riduzione al minimo del trattamento di dati personali mediante misure tecniche e organizzative.

privacy by default

la tutela della protezione del dato deve essere l'impostazione predefinita.

Il titolare deve adottare misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è conforme al regolamento (art. 24).

Tale obbligo vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione, l'accessibilità del dato.

Pseudonimizzazione e minimizzazione quale impostazione predefinita.

principio di responsabilizzazione

(artt. 24, 27, 28, 29)

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative ADEGUATE per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento in modo tale da garantire un livello di sicurezza adeguato al rischio.

Tali misure devono tenere conto dello stato dell'arte, della natura del trattamento, dell'ambito di applicazione, del contesto, delle finalità, dei rischi connessi all'attività svolta.

(ad es.: pseudonimizzazione, cifratura, capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di un ripristino tempestivo; procedure e test periodici).

esempi di violazione di dati

Perdita di dati

Furto di dati (in formato elettronico e cartaceo)

Alterazione di cartelle

Alterazione di documentazione

Invio di dati all'esterno

Intercettazione di dati

Accesso abusivo al sistema

la valutazione di impatto sulla protezione dei dati personali

- **quando è necessaria**: quando la natura, l'oggetto, il contesto e le finalità del trattamento svolto presentano un elevato rischio per i diritti e le libertà delle persone coinvolte. Ad es. è richiesta in particolare nei seguenti casi:
- a) nel caso in cui si verifichi una valutazione sistematica e globale di aspetti relativi a persona fisiche basata su in trattamento automatizzato…
- b) trattamento su larga scala di categorie particolari di dati personali (art. 9 par.1);
- c) sorveglianza sistematica su larga scala di zona accessibile al pubblico.
- **quando deve essere eseguita**: prima di procedere al trattamento;
- **chi coinvolge**: il titolare, gli eventuali responsabili e il DPO

cosa contiene:

- una descrizione sistematica dei trattamenti previsti;

- una valutazione dei rischi per i diritti e le libertà degli interessati;

- le misure previste per affrontare i rischi

- le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento

Riesame: se necessario il titolare procede ad un riesame per valutare se il trattamento svolto sia conforme

le figure previste dal Regolamento

TITOLARE DEL TRATTAMENTO (art. 24)

CONTITOLARE (art. 26)

RESPONSABILE DEL TRATTAMENTO (art. 28)

DESTINATARI

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

CONTITOLARI DEL TRATTAMENTO

PERSONE AUTORIZZATE AL TRATTAMENTO

INTERESSATI

AUTORITA' DI CONTROLLO

Il Responsabile della protezione dei dati personali
(Data Protection Officer - DPO)

La scheda presenta la figura del **Responsabile della protezione dei dati personali** *(Data Protection Officer)* in base al Regolamento Generale sulla Protezione dei Dati, di cui si attende a breve la pubblicazione nella Gazzetta Ufficiale dell'Unione europea. Il testo normativo si fonda sulla **proposta di Regolamento COM(2012)11** concernente la *"tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati"*, come successivamente modificata a seguito degli emendamenti di Parlamento europeo e Consiglio Ue.

QUALI SONO I REQUISITI?

Il Responsabile della protezione dei dati personali, nominato dal titolare del trattamento o dal responsabile del trattamento, dovrà:

1. possedere un'**adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**;
2. adempiere alle sue funzioni in **piena indipendenza** ed in assenza di **conflitti di interesse**;
3. operare **alle dipendenze del titolare o del responsabile** oppure sulla base di **un contratto di servizio**.

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati personali le **risorse umane e finanziarie** necessarie all'adempimento dei suoi compiti.

IN QUALI CASI E' PREVISTO?

Dovranno designare **obbligatoriamente** un **Responsabile della protezione dei dati personali**:

a) **amministrazioni ed enti pubblici**, fatta eccezione per le autorità giudiziarie;

b) tutti i soggetti la cui **attività principale** consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il **controllo regolare e sistematico degli interessati**;

c) tutti i soggetti la cui **attività principale** consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

- Un titolare del trattamento o un responsabile del trattamento possono comunque designare un Responsabile della protezione dei dati personali anche in casi diversi da quelli sopra indicati.
- Un gruppo di imprese o soggetti pubblici possono nominare un **unico Responsabile della protezione dei dati**.

QUALI SONO I COMPITI?

Il Responsabile della protezione dei dati personali dovrà:

a) **informare e consigliare** il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli **obblighi derivanti dal Regolamento europeo** e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) **verificare l'attuazione e l'applicazione del Regolamento**, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli *audit* relativi;

c) **fornire**, se richiesto, **pareri** in merito alla **valutazione d'impatto** sulla protezione dei dati e sorvegliare i relativi adempimenti;

d) **fungere da punto di contatto** per gli **interessati** in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;

e) **fungere da punto di contatto** per il **Garante per la protezione dei dati personali** oppure, eventualmente, consultare il Garante di propria iniziativa.

chi è il DPO?

E’ un soggetto che deve possedere adeguata esperienza, conoscenze della normativa e delle prassi di gestione in materia di trattamento dati personali

E’ un soggetto che opera in totale indipendenza ed autonomia, che si interfaccia direttamente con i vertici aziendali

Può essere un soggetto interno alla struttura, oppure un soggetto esterno

cosa deve fare?

Informare e consigliare il titolare o il responsabile in merito agli obblighi del Regolamento

conservare la documentazione relativa a tale attività ed alle risposte ricevute

sorvegliare e supervisionare l'attuazione e l'applicazione delle procedure e delle misure di sicurezza

Condurre verifiche periodiche

Controllare l'attuazione del regolamento con particolare riguardo alla protezione e alla sicurezza dei dati

Effettuare verifiche periodiche e rilevare e gestire le non conformità

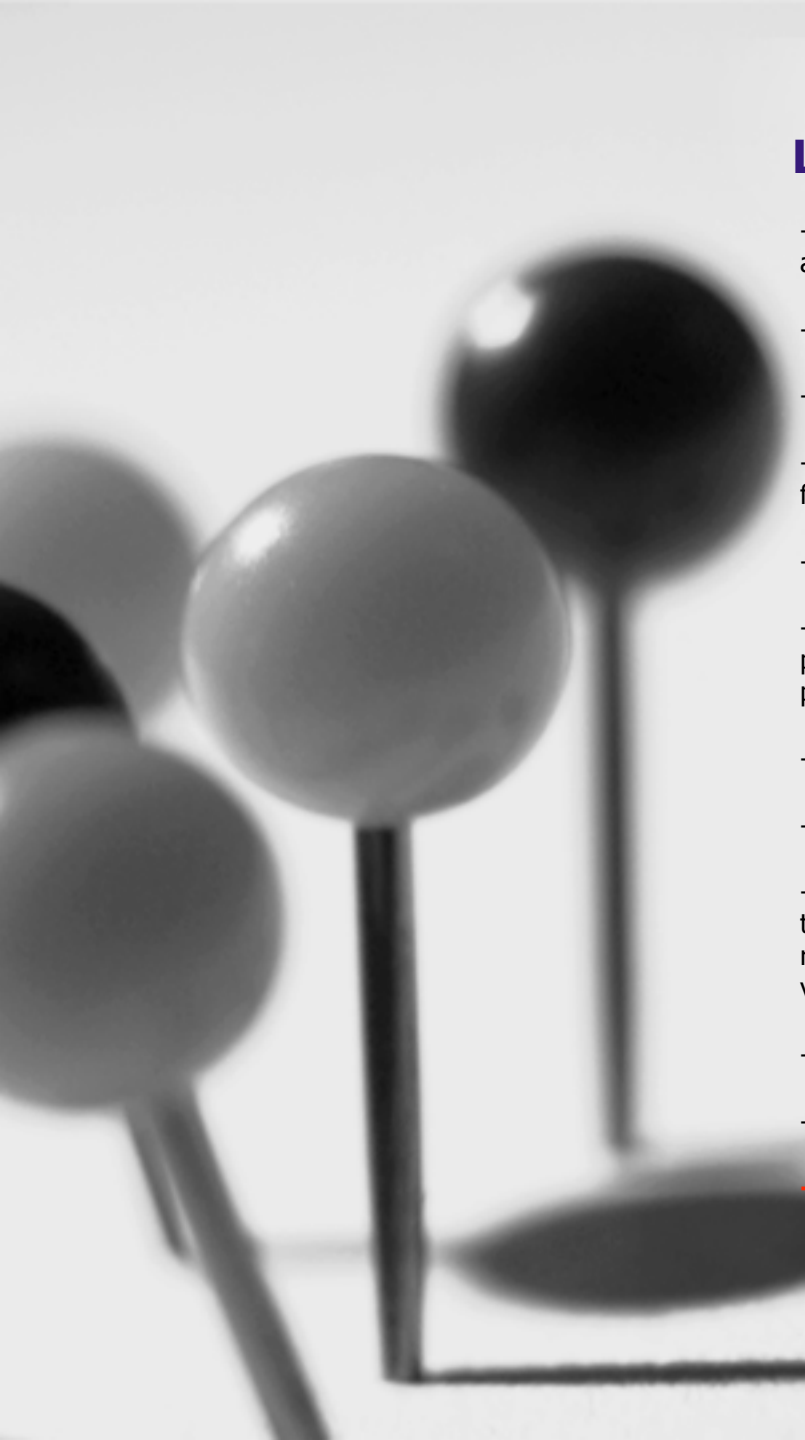
Conservare la documentazione di cui all'art. 28

Controllare che le violazioni ai dati personali siano documentate, notificate e comunicate ai sensi degli art. 31 e 32

Supervisionare il processo di valutazione d'impatto

Controllare che sia dato seguito alle richieste dell'autorità di controllo

Fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento e, se del caso, consultare l'autorità di controllo di propria iniziativa



Linee guida WP 29 13 dicembre 2016

- i DPO non rispondono personalmente in caso di inosservanza del Regolamento. L'onere di assicurare il rispetto della normativa spetta al titolare del trattamento;

- deve disporre di autonomia e risorse sufficienti per svolgere i compiti cui chiamato;

- la designazione può essere formalizzata sia dal titolare che dal responsabile;

- può essere nominato da più soggetti a condizione che sia "facilmente raggiungibile" (sia fisicamente che attraverso mezzi dedicati);

- è vincolato al segreto e alla riservatezza nell'esercizio delle proprie funzioni;

- REQUISITI: essere dotato di "competenze specialistiche" della normativa e delle prassi di protezione dei dati; avere familiarità con le operazioni di trattamento svolte e le misure di protezione adottate dal titolare; rispettare "elevati standard deontologici".

- la funzione può essere esercitata sulla base di un contratto di servizi;

- i dati di contatto del DPO devono essere diffusi e comunicati all'autorità di controllo;

- deve essere coinvolto in tutte le questioni concernenti la protezione dei dati personali e in tutte le valutazioni di impatto sulla protezione dei dati. Dovrebbe partecipare su base regolare alle riunioni del management; deve essere consultato tempestivamente in caso di violazione dei dati o altro incidente;

- deve ricevere le risorse necessarie per assolvere ai propri compiti;

- formazione permanente

-PIENA INDIPENDENZA E AUTONOMIA e ASSENZA DI CONFLITTI DI INTERESSE

I REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

REGISTRO DEL TITOLARE

indicazioni del titolare
finalità del trattamento
descrizione delle categorie di interessati e dei dati trattati
categorie di destinatari cui i dati potranno essere comunicati
termini previsti per la cancellazione delle diverse categorie di dati
descrizione delle misure di sicurezza tecniche e organizzative

REGISTRO DEL RESPONSABILE

dati di contatto del responsabile
categorie dei trattamenti effettuati per conto del titolare
descrizione delle misure di sicurezza tecniche e organizzative

LA SICUREZZA DEI DATI

Il regolamento prevede misure di sicurezza adeguate da adottare sulla base di una valutazione dei rischi (vedi desiderata n.78).

Il titolare deve:

1) compiere una valutazione dei rischi (distruzione, perdita, modifica, rivelazione, accesso non autorizzato) inerenti al trattamento. Se il rischio è elevato il titolare deve compiere una valutazione di impatto sulla protezione di tale rischio.

2) realizzare le misure per limitare tali rischi (ad es. pseudonimizzazione, cifratura, ecc.)

3) **consultare preventivamente l'autorità di controllo** nel caso in cui dalla valutazione di impatto dovesse emergere che il rischio non potrà essere ragionevolmente attenuato mediante l'adozione delle misure di sicurezza di cui dispone.

considerato n. 78

La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.

DATA BREACH

Non appena il titolare viene a conoscenza di un'avvenuta violazione di dati personali trattati è tenuto a notificare la violazione stessa all'autorità di controllo competente, senza ingiustificato ritardo, entro 72 ore dal momento in cui ne è venuto a conoscenza (art. 33).

La notifica deve descrivere la natura della violazione, i dati del responsabile, le conseguenze della violazione, le misure in atto o quelle in fase di adozione.