Avv. Ernesto Belisario

GDPR- COS'È E PERCHÉ INTERESSA LA PUBBLICA AMMINISTRAZIONE?

www.lapadigitale.it

SOMMARIO

- Dal Codice Privacy al GDPR
- L'ambito di applicazione del GDPR
- I ruoli previsti dal GDPR
- I princìpi del GDPR

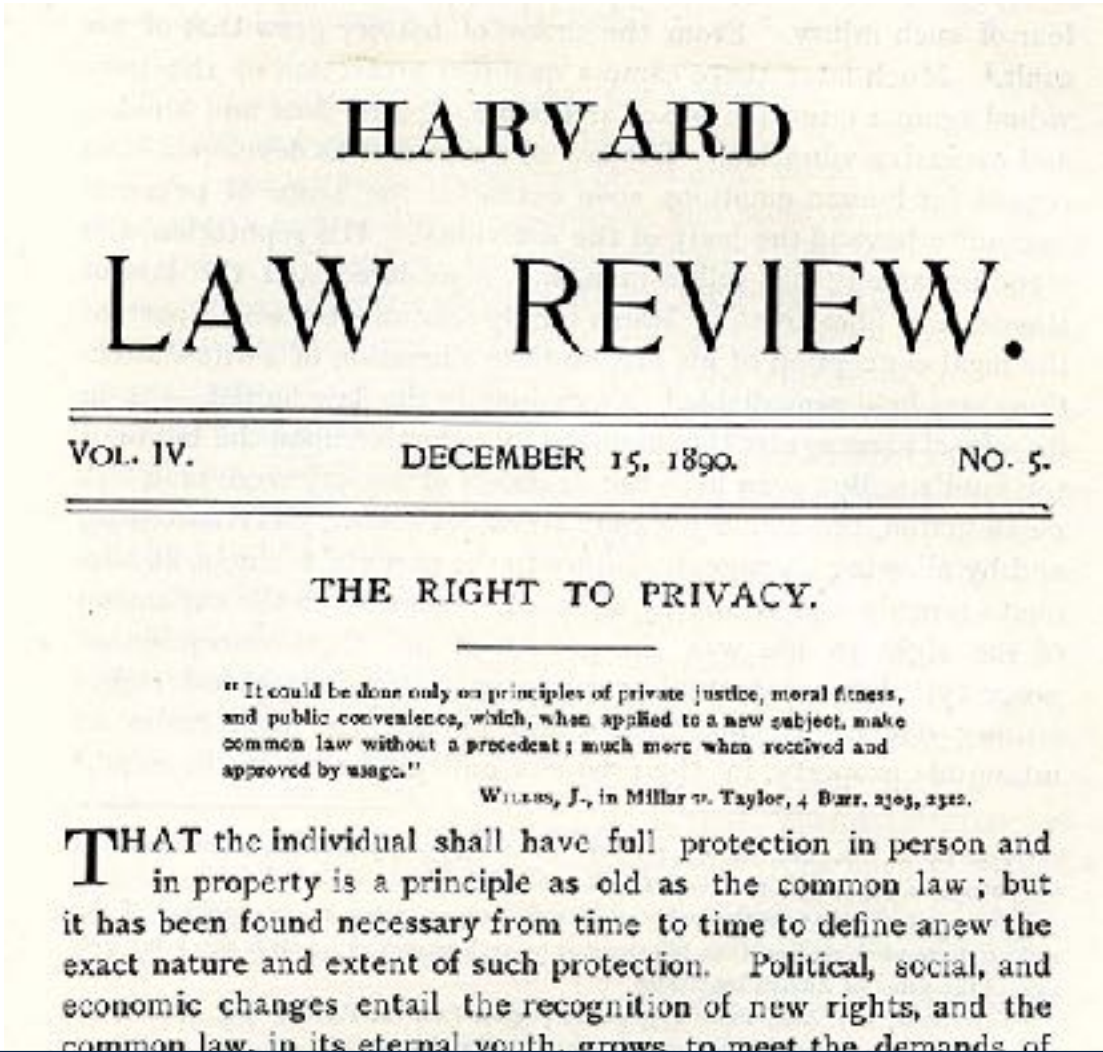
PER INIZIARE…

"La privacy è fin dall'origine collegata alle forme moderne di comunicazione e nasce come diritto dell'eta dell'oro della borghesia, che si costruisce un suo spazio privato circondato da difese, così come si era costruita il suo spazio fisico con il diritto di proprietà. Con le banche dati, le reti, la tv via cavo e anche le tecnologie genetiche - che sono in gran parte raccolte di informazioni sulle persone - il diritto di privacy non è più soltanto quello di essere lasciato solo, ma anche, e soprattutto, quello di controllare il destino delle informazioni che circolano sul proprio conto."

Stefano Rodotà

I - DAL CODICE PRIVACY AL GDPR

DA DOVE SIAMO PARTITI



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

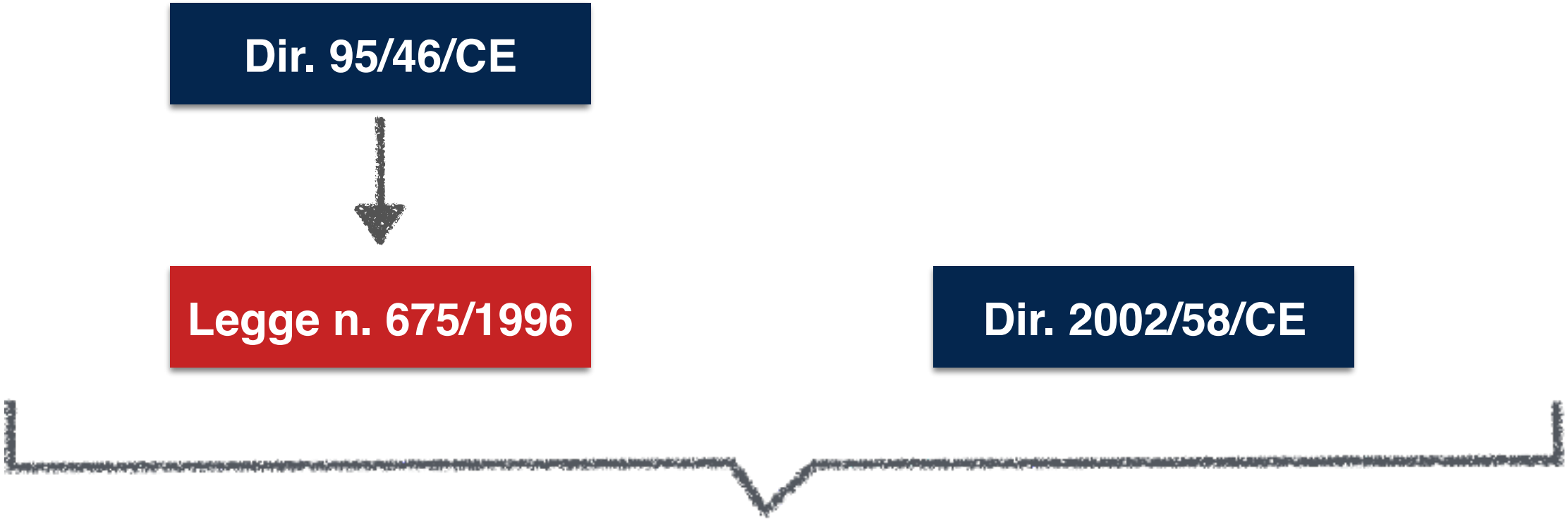
THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

L'EVOLUZIONE DELLA NORMATIVA



Codice Privacy - D. Lgs. n. 196/2003

GENERAL DATA PROTECTION REGULATION

Gazzetta ufficiale L 119

dell'Unione europea

Edizione in lingua italiana

Legislazione

59° anno

4 maggio 2016

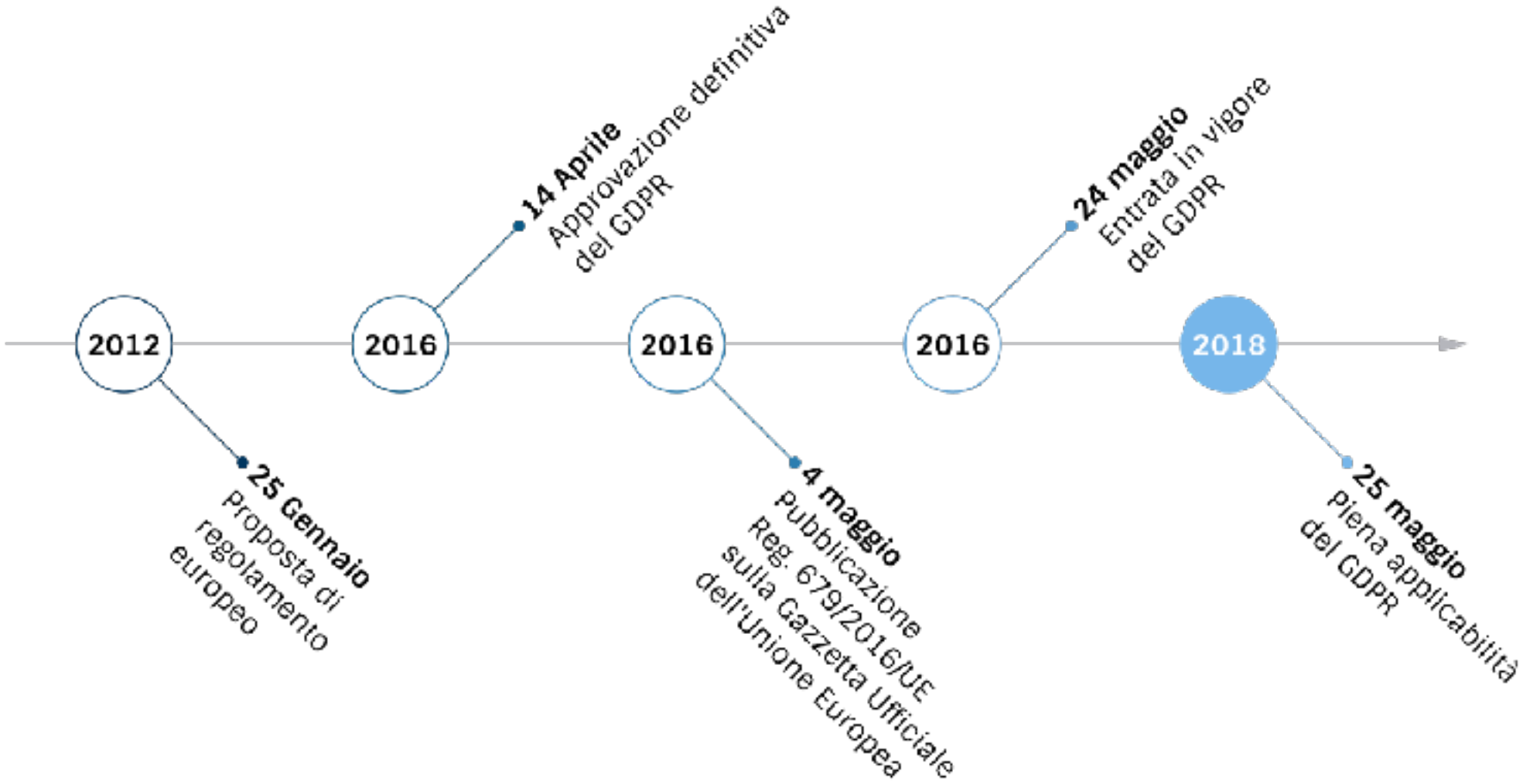
Sommario

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)** (1) 1

IL REGOLAMENTO UE 679/2016



PERCHÈ UN REGOLAMENTO?

La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

Considerando 6 GDPR

UN'UNICA LEGGE UE SULLA PRIVACY

- Le direttive europee sulla privacy miravano all'armonizzazione
- Il Regolamento non necessita di trasposizione
- Il GDPR è un unico testo per tutti gli Stati membri dell'UE
- Alcuni settori restano al di fuori dell'ambito di applicazione del GDPR
- Permane un (limitato) potere legislativo degli Stati membri in materia di protezione dei dati personali
- Viene assegnato un ruolo rilevante alle c.d. "autorità di controllo" (Garanti nazionali)


25th of May
2018

II - L'AMBITO DI APPLICAZIONE DEL GDPR

OGGETTO E FINALITA' DEL GDPR

Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

Art. 1, par. 1, GDPR

AMBITO DI APPLICAZIONE MATERIALE

Il GDPR si applica

- [x] alle persone fisiche e al trattamento interamente o parzialmente automatizzato dei dati personali e al trattamento non automatizzato di dati contenuti in archivio o destinati a figurarvi.

Non si applica, invece:

- [ ] ai trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
- [ ] ai dati anonimi.

AMBITO DI APPLICAZIONE TERRITORIALE

Il Regolamento si applica:

- al trattamento dei dati effettuati nell'ambito delle attività di uno stabilimento situato nell'Unione;
- a quei titolari e responsabili che, pur non avendo uno stabilimento nel territorio dell'Unione, svolgono attività di trattamento dei dati personali di interessati che si trovano nell'Unione, quando le attività riguardino:
  - offerta di beni o prestazione di servizi, anche gratuiti;
  - monitoraggio del comportamento dei soggetti interessati all'interno dell'Unione.

DATO PERSONALE

qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

Art. 4, par. 1, GDPR

CATEGORIE PARTICOLARI DI DATI PERSONALI

dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Art. 9, par. 1, GDPR

CATEGORIE PARTICOLARI DI DATI PERSONALI

«dati genetici»: *i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*

«dati biometrici»: *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;*

«dati relativi alla salute»: *i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;*

Art. 4, par. 1, GDPR

DATI RELATIVI A CONDANNE PENALI E REATI

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Art. 10, par. 1, GDPR

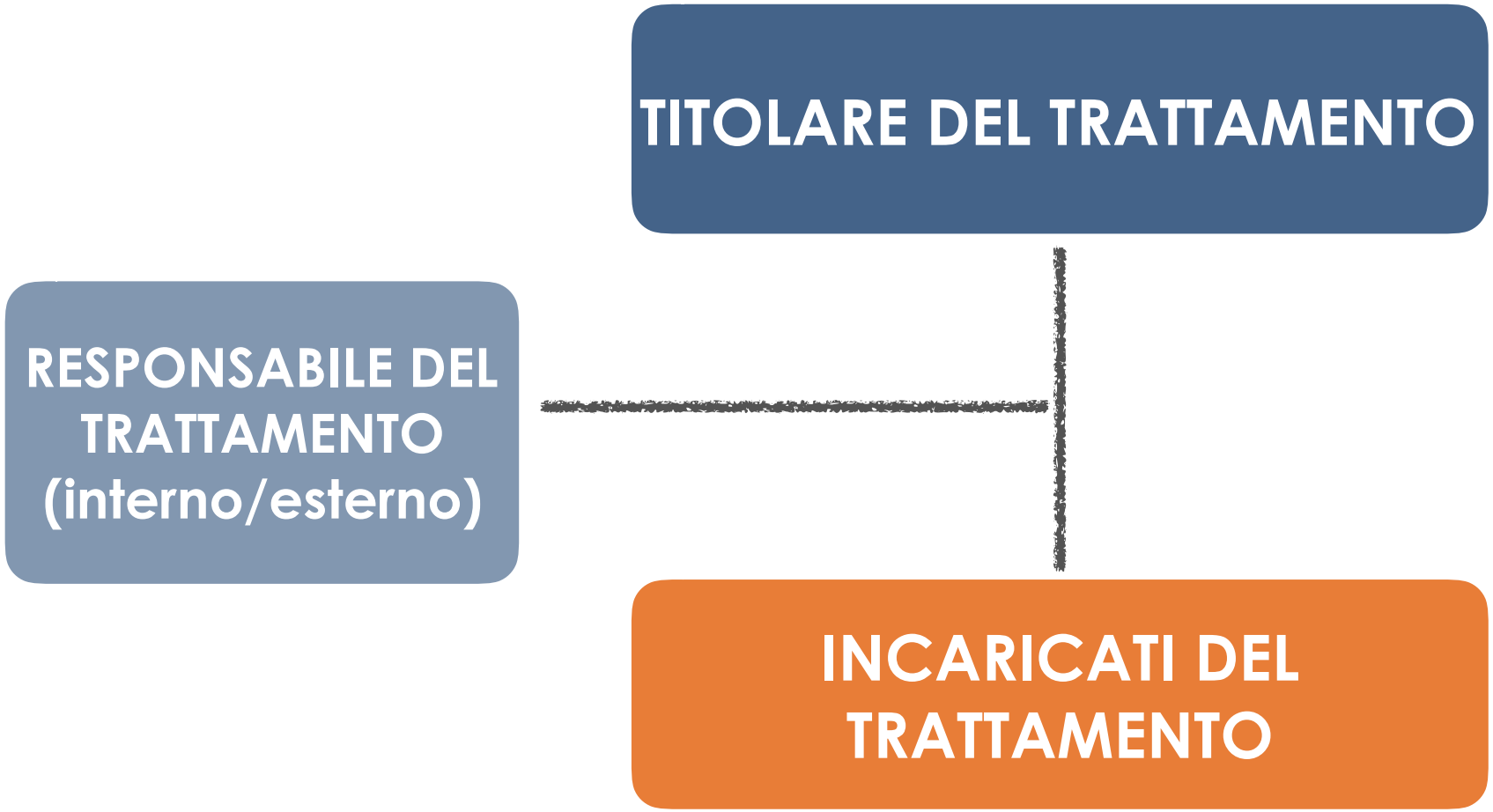
TRATTAMENTO

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 la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Art. 4, par. 1, GDPR

III- I RUOLI PREVISTI DAL GDPR

CODICE PRIVACY



GDPR

TITOLARE DEL TRATTAMENTO

RESPONSABILE DEL TRATTAMENTO (esterno)

RESPONSABILE DELLA PROTEZIONE DEI DATI

AUTORIZZATI AL TRATTAMENTO

SUB-RESPONSABILE

TITOLARE DEL TRATTAMENTO

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Art. 4, par. 1, GDPR

RESPONSABILE DEL TRATTAMENTO

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Art. 4, par. 1, GDPR

RESPONSABILE DEL TRATTAMENTO

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Art. 28, par. 1, GDPR

RESPONSABILE DEL TRATTAMENTO

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Art. 28, par. 3, GDPR

RESPONSABILE DEL TRATTAMENTO

- *trattare i dati personali soltanto su istruzione documentata del titolare del trattamento;*
- *garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;*
- *adottare le misure di sicurezza;*
- *rispettare i limiti previsti per la nomina dei sub-responsabili;*
- *assistere il titolare del trattamento in relazione all'esercizio dei diritti degli interessati;*
- *cancellare o restituire al titolare tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti;*
- *mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.*

Art. 28, par. 3, GDPR

RESPONSABILE PROTEZIONE DATI

QUANDO È OBBLIGATORIO IL DPO

La designazione del DPO è obbligatoria (da parte del Titolare o del Responsabile del trattamento) solo se:

1. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali;

2. le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

3. le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'art. 9 o 10 GDPR.

COMPITI DEL DPO

- Informare e fornire al Titolare, al Responsabile nonché ai dipendenti che eseguono il trattamento, consulenza in merito agli obblighi normativi in materia;

- Sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle politiche in materia del Titolare o del Responsabile del trattamento, compresi l'attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa al trattamento e al controllo in merito;

- Fornire, se richiesto, pareri sulla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

- Cooperare con l'Autorità di controllo e fungere da punto di contatto con il Garante per la protezione dei dati di personali per questioni connesse al trattamento.

IL RUOLO DEL DPO

- ☑ Il DPO va designato in funzione delle qualità professionali, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti.

- ☑ È figura apicale, assolutamente diversa quanto a ruolo e funzioni dal "semplice" responsabile del trattamento.

- ☑ Può essere un dipendente del Titolare o del Responsabile del trattamento oppure un consulente esterno che assolve i suoi compiti in base a un contratto di servizi.

- ☑ I dati di contatto del DPO vanno comunicati al Garante per la protezione dei dati personali e resi pubblici.

IL RUOLO DEL DPO

Il DPO deve essere autonomo ed indipendente:

- non deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati né è soggetto a potere disciplinare o sanzionatorio per l'adempimento dei propri compiti.
- deve avere le risorse necessarie e il potere di spesa per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).

IL DPO E GLI INTERESSATI

Il RPD, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa.
Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

(Linee Guida Gruppo Art. 29)

RESPONSABILITA' DEL DPO

I DPO non rispondono personalmente in caso di inosservanza del GDPR. Quest'ultimo chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile.

(Linee Guida Gruppo Art. 29)

GESTIONE IN FORMA ASSOCIATA

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

(Art. 37, par. 3, GDPR)

DPO INTERNO

- Nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

- Necessario apposito atto di designazione

DPO ESTERNO

- Nel caso dei DPO esterno, le funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica. Se la funzione di DPO è svolta da un fornitore esterno di servizi, i compiti stabiliti per il DPO potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale DPO soddisfi tutti i requisiti applicabili come fissati nel GDPR.

- Necessario fare attenzione alla procedura di evidenza per la scelta del DPO (valore affidamento, requisiti partecipanti, SLA contratto)

AUTORITA' DI CONTROLLO

Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).

(Art. 51, par. 1, GDPR)

IV- I PRINCIPI DEL GDPR

PRINCIPI APPLICABILI AL TRATTAMENTO

I dati personali sono

- ☑ trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
- ☑ raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali (limitazione della finalità);
- ☑ conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

PRINCIPI APPLICABILI AL TRATTAMENTO

I dati personali sono

- ☑ adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
- ☑ esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);
- ☑ trattati in maniera 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 (integrità e riservatezza).

PRINCIPIO DI ACCOUNTABILITY

Il titolare del trattamento è competente per il rispetto dei principi previsti dal GDPR e in grado di comprovarlo (c.d principio di «responsabilizzazione»).

(Art. 5, par. 2, GDPR)

LICEITA' DEL TRATTAMENTO

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è 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;
f)il trattamento è necessario per il perseguimento del legittimo interesse 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.

PRIVACY BY DESIGN

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Art. 25, par. 1 GDPR

PRIVACY BY DEFAULT

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Art. 25, par. 2 GDPR

SOMMARIO

- I diritti dell'interessato
- I principali adempimenti
- Il GDPR e l'attività amministrativa
- Il sistema sanzionatorio del GDPR

PER INIZIARE…

"Quando si tratta di privacy e di responsabilità, le persone chiedono sempre la prima per sé e la seconda per tutti gli altri. "

David Brin

I - I DIRITTI DELL'INTERESSATO

I DIRITTI AL CENTRO

Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento.

Considerando 39 GDPR

I DIRITTI AL CENTRO

In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

Considerando 39 GDPR

IL SISTEMA DEI DIRITTI INDIVIDUALI

ACCESSO

INFORMATIVA

CANCELLAZIONE

RETTIFICA

PORTABILITA’

LIMITAZIONE

OPPOSIZIONE

PROCESSO DECISIONALE AUTOMATIZZATO

IL SISTEMA DEI DIRITTI INDIVIDUALI

ACCESSO

INFORMATIVA

CANCELLAZIONE

RETTIFICA

PORTABILITA'

LIMITAZIONE

OPPOSIZIONE

PROCESSO DECISIONALE AUTOMATIZZATO

TRASPARENZA

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.
Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.
Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Art. 12, par. 1, GDPR

LA "NUOVA" INFORMATIVA

- Rispetto all'art. 13 del Codice Privacy, si prevedono numerose informazioni aggiuntive da fornire agli interessati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

- L'Informativa va resa per iscritto o con altri mezzi, anche elettronici.

- Anche oralmente, purché sia richiesto dall'interessato e sia comprovata con altri mezzi l'identità dell'interessato.

- Le informazioni possono essere fornite anche in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone devono essere leggibili da qualsiasi dispositivo.

LA "NUOVA" INFORMATIVA

Rispetto agli elementi obbligatori da indicare nell'informativa privacy ai sensi dell'art. 13 del Codice Privacy, i Titolari del trattamento dovranno inserire obbligatoriamente anche le seguenti informazioni a:

- i dati di contatto del DPO;
- la base giuridica del trattamento a corredo della illustrazione delle finalità del trattamento;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- il diritto di proporre reclamo al Garante per la protezione dei dati personali.

RACCOMANDAZIONI

Il regolamento supporta chiaramente il concetto di informativa "stratificata".

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

IL CONSENSO

qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento

(Art. 4, par. 1, GDPR)

IL SISTEMA DEI DIRITTI INDIVIDUALI

ACCESSO

INFORMATIVA

CANCELLAZIONE

RETTIFICA

PORTABILITA'

LIMITAZIONE

OPPOSIZIONE

PROCESSO DECISIONALE AUTOMATIZZATO

DIRITTO DI ACCESSO

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

Art. 15, par. 1, GDPR

DIRITTO DI ACCESSO

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Art. 15, par. 1, GDPR

RACCOMANDAZIONI

I titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

IL SISTEMA DEI DIRITTI INDIVIDUALI

ACCESSO

INFORMATIVA

CANCELLAZIONE

RETTIFICA

PORTABILITA'

LIMITAZIONE

OPPOSIZIONE

PROCESSO DECISIONALE AUTOMATIZZATO

DIRITTO DI ACCESSO

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Art. 16, par. 1, GDPR

IL SISTEMA DEI DIRITTI INDIVIDUALI

ACCESSO

INFORMATIVA

CANCELLAZIONE

RETTIFICA

PORTABILITA’

LIMITAZIONE

OPPOSIZIONE

PROCESSO DECISIONALE AUTOMATIZZATO

DIRITTO ALL'OBLIO

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo quando:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Art. 17, par. 1, GDPR

IL SISTEMA DEI DIRITTI INDIVIDUALI

ACCESSO

INFORMATIVA

CANCELLAZIONE

RETTIFICA

PORTABILITA'

LIMITAZIONE

OPPOSIZIONE

PROCESSO DECISIONALE AUTOMATIZZATO

DIRITTO DI LIMITAZIONE

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Art. 18 GDPR

COSA CAMBIA

- Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), 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(in attesa della valutazione da parte del titolare).

- Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato

RACCOMANDAZIONI

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori; pertanto, è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

IL SISTEMA DEI DIRITTI INDIVIDUALI

ACCESSO

INFORMATIVA

CANCELLAZIONE

RETTIFICA

PORTABILITA'

LIMITAZIONE

OPPOSIZIONE

PROCESSO DECISIONALE AUTOMATIZZATO

DIRITTO ALLA PORTABILITA'

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b) il trattamento sia effettuato con mezzi automatizzati.

Art. 20, par. 1, GDPR

DIRITTO ALLA PORTABILITA'

Tale diritto non si applica al 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.

Art. 20, par. 3, GDPR

MODALITA' DI ESERCIZIO DEI DIRITTI

COSA CAMBIA

- Il termine per la risposta all'Interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità;

- Il Titolare deve comunque dare un riscontro all'Interessato entro 1 mese dalla richiesta, anche in caso di diniego;

- spetta al titolare valutare la complessità del riscontro all'Interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'Interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive.

COSA CAMBIA

- Il riscontro all'Interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità;

- Può essere dato oralmente solo se così richiede l'Interessato;

- La risposta fornita all'Interessato non deve essere solo"intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

COSA RESTA INVARIATO

- Il Titolare del Trattamento deve agevolare l'esercizio dei diritti da parte dell'Interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea;
- Benché sia il solo Titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati;
- L'esercizio dei diritti è, in linea di principio, gratuito per l'Interessato, ma possono esservi eccezioni;
- Il Titolare ha il diritto di chiedere informazioni necessarie a identificare l'Interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.

II - I PRINCIPALI ADEMPIMENTI PER LE PA

ADEMPIMENTI ORGANIZZATIVI

- ☑ Adeguamento dell'organizzazione della PA al GDPR (definizione dell'ufficio competente per adempimenti, predisposizione istruzioni agli uffici e ai soggetti autorizzati);

- ☑ Individuazione e nomina del DPO;

- ☑ Adeguamento delle nomine dei responsabili esterni.

DIRITTI DEGLI INTERESSATI

- ☑ Revisione e integrazione delle informative;
- ☑ Revisione modalità con cui gli interessati esprimono il consenso.

VALUTAZIONE D'IMPATTO

Le amministrazioni dovranno effettuare una Valutazione degli impatti privacy (Privacy Impact Assessment– PIA) fin dal momento della progettazione del processo amministrativo e degli applicativi informatici di supporto, nei casi in cui il trattamento alla base degli stessi, per sua natura, oggetto o finalità, presenti rischi specifici per i diritti e le libertà degli interessati.

(Art. 35 GDPR)

VALUTAZIONE D'IMPATTO

La valutazione contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

(Art. 35, par. 7, GDPR)

VALUTAZIONE D'IMPATTO

Il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

(Considerando 84 GDPR)

ADEMPIMENTI PER LA SICUREZZA

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
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.

(Art. 32, par. 1, GDPR)

MISURE DI SICUREZZA

- Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare 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.

- Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento.

PSEUDONIMIZZAZIONE

il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

(Art. 4 GDPR)

REGISTRO DEI TRATTAMENTI

Ogni titolare del trattamento tiene un registro elettronico in cui sono riportate le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, 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;

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.

(Art. 30, par. 1, GDPR)

ADEMPIMENTI PER DATA BREACH

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

(Art. 33, par. 1, GDPR)

DATA BREACH

la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

(Art. 4, par. 1, GDPR)

ADEMPIMENTI PER DATA BREACH

La notifica deve almeno:

- ☑ *descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;*
- ☑ *comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*
- ☑ *descrivere le probabili conseguenze della violazione dei dati personali;*
- ☑ *descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

(Art. 33, par. 3, GDPR)

III - IL GDPR E L'ATTIVITÀ AMMINISTRATIVA

LA DIGITALIZZAZIONE DEI DOCUMENTI E DEGLI ARCHIVI E L'EVOLUZIONE DEI SISTEMI INFORMATIVI DELL'AMMINISTRAZIONE

GDPR E TRASPARENZA AMMINISTRATIVA

I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento.

(Art. 86, par. 1, GDPR)

GDPR E TRASPARENZA AMMINISTRATIVA

Le amministrazioni devono

- ☑ fare attenzione al contenuto delle motivazioni degli atti;
- ☑ verificare la non eccedenza delle informazioni pubblicate rispetto a quanto previsto dalle norme;
- ☑ verificare che i dati e documenti vengano pubblicati solo per il periodo individuato dalla normativa (con le dovute differenze a seconda che si tratti di diffusione per pubblicità legale o per trasparenza).

GDPR E VIDEOSORVEGLIANZA

Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala.

(Considerando 91 GDPR)

IV - IL SISTEMA SANZIONATORIO DEL GDPR

IL SISTEMA SANZIONATORIO

Il GDPR definisce un impianto sanzionatorio molto più rigido di quello previsto dal Codice Privacy:

- ☑ sono previste sanzioni amministrative fino a 20 milioni di Euro;
- ☑ è prevista la responsabilità civile nei confronti dell'interessato che subisca un danno materiale o immateriale causato da una violazione del GDPR;
- ☑ sanzioni penali possono essere previste dal legislatore nazionale.

SANZIONI AMMINISTRATIVE

fino a 20 milioni di euro, in caso di violazione delle disposizioni in materia di:

- principi di base del trattamento, comprese le condizioni relative al consenso;
- diritti degli interessati;
- trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

SANZIONI AMMINISTRATIVE

fino a 10 milioni di euro, in caso di violazione delle disposizioni in materia di:

- obblighi del titolare del trattamento e del responsabile del trattamento;
- obblighi dell'organismo di certificazione;
- obblighi dell'organismo di controllo.

PRINCIPIO DI PROPORZIONALITA'

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- il carattere doloso o colposo della violazione;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

PRINCIPIO DI PROPORZIONALITA'

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto;
- eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

PRINCIPIO DI PROPORZIONALITA'

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- le categorie di dati personali interessate dalla violazione;
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- qualora siano stati precedentemente disposti provvedimenti nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

PRINCIPIO DI PROPORZIONALITA'

Le sanzioni amministrative sono comminate dall'autorità di controllo sulla base delle seguenti circostanze (art. 53, par. 2, GDPR):

- l'adesione ai codici di condotta approvati ai sensi dell'articolo o ai meccanismi di certificazione;

- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

PROFILI RISARCITORI

Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

Art. 82, par. 1, GDPR

PROFILI RISARCITORI

Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Art. 82, par. 2 e 3, GDPR

RESPONSABILITA' ERARIALE

La responsabilità erariale sussiste, inoltre, in tutti i casi in cui le nuove tecnologie siano utilizzate in modo scorretto: basti pensare alla mancata adozione delle cautele di sicurezza previste dalla normativa in materia di riservatezza di dati personali (artt. 31 ss, d.lgs. n. 196/2003) che abbia determinato un risarcimento al privato danneggiato, oppure l'assenza di procedure di controllo che abbia determinato un danno diretto alle casse dell'Ente

Corte Conti, Reg. Toscana, 26 aprile 2006, n. 265

GRAZIE PER L'ATTENZIONE

www.lapadigitale.it