AReSS
Agenzia Regionale per la Salute ed il Sociale
Regione Puglia

I manuali del RTD

Privacy e protezione dati personali

VERSIONE 1.0

28/03/2025

SOMMARIO

Indice delle figure

Versioni del documento

Versione	data	Modifiche
1.0	28/03/2025	Prima versione del documento.

Autori del documento

Dott. Vito Petrarolo

Dirigente Servizio Transizione Digitale e Privacy, Responsabile per la Transizione al Digitale

Dott. Pasquale Notarangelo

Dott. Simone Pisanò

Dott.ssa Laura Scaringella

Con la supervisione del DPO

Dott. Nicola Parisi

Con la consulenza di

Avv. Giovanni Maglio

Email to: **rtd@aress.regione.puglia.it**

QUADRO GIURIDICO IN MATERIA DI PRIVACY E PROTEZIONE DEI DATI PERSONALI

Introduzione

Il tema della privacy e della protezione dei dati personali è diventato negli ultimi anni sempre più rilevante e di grande impatto sulle vite di tutti, non solo da un punto di vista personale e lavorativo, ma anche come singoli individui e componenti della società nel suo insieme.

Occorre partire, però, da una precisazione, ossia che il diritto al rispetto della vita privata (privacy) e il diritto alla protezione dei dati personali, anche se nel corso del tempo la differenza si è affievolita e spesso le due tematiche si sovrappongo, sono diritti distinti tra di loro, sebbene strettamente legati, in quanto mirano a proteggere valori simili (ad es. la dignità umana), garantendo un ambito personale nel quale poter sviluppare, senza condizionamenti, la personalità, le opinioni e, conseguentemente, il proprio modo di agire.
Da questo punto di vista, rappresentano un presupposto essenziale per l'esercizio di altre libertà fondamentali, quali la libertà di parola, la libertà di riunione pacifica e di associazione, e la libertà di religione.

Inoltre, i due diritti hanno una diversa formulazione e portata; infatti, mentre la privacy è un generale divieto di ingerenza da parte di soggetti estranei, eventualmente ed eccezionalmente limitato da alcune esigenze di interesse pubblico, la protezione dei dati personali è un sistema di trattamento degli stessi che identifica direttamente o indirettamente una persona e prevede un insieme organizzato di controlli e bilanciamenti volti a proteggere le persone fisiche ogni qualvolta siano trattati i loro dati personali.

Storicamente la privacy viene fatta risalire alla fine del 1800 (1890), allorquando due giuristi americani – Warren e Brandeis - scrissero un articolo intitolato "*The Right To Privacy*", dove si teorizzava il "*right to be let alone*", ossia il diritto alla vita privata, conosciuto nel diritto europeo come diritto al rispetto della vita privata, che è stato sancito dalla **dichiarazione universale dei diritti dell'uomo (UDHR)**, adottata nel 1948, come uno dei diritti umani fondamentali protetti.

Poco dopo l'adozione di tale dichiarazione, anche l'Europa ha sancito questo diritto, nella **Convenzione europea dei diritti dell'uomo (CEDU)**, un trattato giuridicamente vincolante per le parti contraenti, redatto nel 1950. La CEDU stabilisce che ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. L'ingerenza di un'autorità pubblica in questo diritto è vietata, eccetto nei casi in cui sia prevista dalla legge, persegua interessi pubblici importanti e legittimi e sia necessaria in una società democratica.

1 Quadro europeo

La Carta dei diritti fondamentali dell'UE (art. 8) e l'**art. 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE)** stabiliscono che tutti i cittadini dell'UE hanno diritto alla protezione dei propri dati personali. Tali dati devono essere trattati secondo correttezza, per finalità determinate e sulla base del consenso dell'interessato o di altro fondamento legittimo previsto dalla legge. Ciascuno ha, inoltre, il diritto di accesso ai dati raccolti che lo riguardano e il diritto alla rettifica degli stessi.

A seguito di tali atti di altissimo livello, il Regolamento generale sulla protezione dei dati (**Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016** sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati (GDPR), e che abroga la **Direttiva 95/46/CE**, c.d. GDPR), applicabile dal 25 maggio 2018, rafforza il diritto dell'individuo alla protezione dei dati personali, riflettendo la natura della protezione dei dati come diritto fondamentale per l'Unione Europea.

Il GDPR prevede un insieme unico di norme direttamente applicabili in tutti gli ordinamenti giuridici degli Stati membri e garantisce la libera circolazione dei dati personali tra gli Stati membri dell'UE, migliorando così anche le opportunità commerciali.

Ai sensi dell'**art. 2**, il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio[1] o destinati a figurarvi.

Il **paragrafo 2 dell'art. 2** stabilisce alcune esenzioni: Il GDPR, infatti, non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del **titolo V, capo 2, TUE**[2];
c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Per quanto riguarda l'ambito di applicazione territoriale, il Regolamento si applica al trattamento dei dati personali nell'ambito delle attività di uno stabilimento di un titolare o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento abbia luogo o meno nell'Unione.
Inoltre, si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Definizioni

Innanzitutto, occorre chiarire il significato di alcuni termini, ai sensi dell'**art. 4**:

"**dati personali**": qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"); una persona fisica identificabile è una persona che può essere identificata, direttamente o

[1] Art. 4 par. 1 n. 6) «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;
[2] Politica estera e sicurezza comune.

indirettamente, in particolare mediante riferimento a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o a uno o più fattori specifici dell'aspetto fisico, fisiologico, identità genetica, mentale, economica, culturale o sociale di quella persona fisica;

Tra i dati personali ci sono diverse tipologie, in particolare le seguenti, rilevanti nel settore sanitario:

"**dati relativi alla salute**": i dati personali relativi alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi sanitari, che rivelano informazioni sul suo stato di salute.

In base al **Considerando 35**, nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla **direttiva 2011/24/UE** del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

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

"**dati biometrici**": i dati personali risultanti da un trattamento tecnico specifico relativo alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che consentono o confermano l'identificazione univoca di tale persona fisica, come immagini facciali o dati dattiloscopici.

Un'altra categoria di dati delicati è quella dei dati giudiziari.

L'**art. 10** GDPR, infatti, relativo al Trattamento dei dati personali relativi a condanne penali e reati, stabilisce che 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.

Infine, per «**trattamento**» s'intende 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.

I principi

L'**art. 5**, poi, stabilisce alcuni principi fondamentali per un corretto e lecito trattamento dei dati personali, che dovrebbero essere:

(a) trattati in modo lecito, secondo correttezza e in modo trasparente nei confronti dell'interessato (**principio di liceità, correttezza e trasparenza**);

(b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità; l'ulteriore trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ai sensi dell'**art. 89, paragrafo 1**, non è da considerarsi incompatibile con le finalità iniziali (**principio della limitazione delle finalità**);

(c) adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati (**principio di minimizzazione dei dati**);

(d) esatti e, ove necessario, aggiornati; ogni ragionevole misura deve essere adottata per garantire che i dati personali inesatti, rispetto alle finalità per le quali sono trattati, siano cancellati o rettificati senza indugio (**principio di esattezza**);

(e) conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario alle finalità per le quali i dati personali sono trattati; i dati personali possono essere conservati per periodi più lunghi nella misura in cui i dati personali saranno trattati esclusivamente a fini di archiviazione nel pubblico interesse, a fini di ricerca scientifica o storica o a fini statistici ai sensi dell'**art. 89, paragrafo 1**, previa attuazione di adeguate disposizioni tecniche e organizzative, misure previste dal presente Regolamento al fine di tutelare i diritti e le libertà dell'interessato (**principio della limitazione della conservazione**);

(f) trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro trattamenti non autorizzati o illeciti e contro la perdita, la distruzione o il danneggiamento accidentali, utilizzando misure tecniche o organizzative adeguate (**principio di integrità e riservatezza**).

Ultimo principio, ma non per importanza, è il principio di responsabilità che afferma che il titolare del trattamento è responsabile e può dimostrare il rispetto di tutti gli altri principi sopra elencati (**accountability**).

Privacy by design e privacy by default

Un altro paio di principi importanti sono quelli dell'**art. 25**, ove si precisa che tenuto conto dello stato della tecnica, dei costi di attuazione e della natura, dell'ambito, del contesto e delle finalità del trattamento nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche posti dal trattamento, il titolare del trattamento deve, sia al momento della determinazione dei mezzi per il trattamento che al momento del trattamento stesso, adottare misure tecniche e organizzative adeguate, come la pseudonimizzazione, che sono volte ad attuare i principi di protezione dei dati, come minimizzazione dei dati, in modo efficace e per integrare le garanzie necessarie nel trattamento al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati. Questi principi sono, rispettivamente, chiamati **Privacy by design e Privacy by default**.

Anche il **Considerando 78** del GDPR afferma che i titolari del trattamento dovrebbero adottare politiche interne e attuare misure che soddisfino, in particolare, i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita al fine di dimostrare la conformità con il GDPR stesso.

Le basi giuridiche

In esecuzione del principio di liceità, l'**art. 6** prevede che ogni attività di trattamento debba essere svolta solo su base giuridica.

Base giuridica per la liceità del trattamento dei dati personali, di cui all'art. 6, sono:

a) il consenso[3] al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte o per porre in essere provvedimenti su richiesta dell'interessato prima della conclusione di un contratto;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per le finalità dei legittimi interessi[4] perseguiti dal titolare del trattamento o da terzi, salvo che su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare laddove il soggetto sia un minore.

Si precisa che l'ultima base giuridica non si applica ai trattamenti effettuati dalle pubbliche autorità nell'espletamento dei propri compiti.

In genere, come prescritto dall'**art. 9**, che si riferisce a dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché al trattamento di dati genetici, dati biometrici al fine di identificare in modo univoco una persona fisica, dati relativi alla salute o dati riguardanti la vita sessuale o l'orientamento sessuale di una persona fisica, è vietato trattare questo tipo di categorie particolari di dati.

Tuttavia, questa prescrizione non si applica se:

(a) l'interessato ha espresso il proprio consenso al trattamento di tali dati personali per una o più finalità determinate, salvo che il diritto dell'Unione o degli Stati membri preveda che il divieto di cui sopra non possa essere revocato dall'interessato;
(b) il trattamento è necessario per l'adempimento degli obblighi e per l'esercizio di specifici diritti del titolare o dell'interessato in materia di diritto del lavoro e previdenziale e di protezione sociale nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri che preveda garanzie adeguate per i diritti fondamentali e gli interessi dell'interessato;
(c) il trattamento è necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica qualora l'interessato sia fisicamente o giuridicamente incapace di prestare il consenso;

[3] Art. 4 par. 1 n. 11) «consenso dell'interessato»: 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.
Al riguardo si vedano anche le Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679
Versione 1.1 adottate il 4 maggio 2020 dal EDPB
[4] Si veda il Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE del WP29

(d) il trattamento è svolto nel corso delle sue legittime attività con garanzie adeguate da una fondazione, associazione o altro ente senza scopo di lucro aventi finalità politiche, filosofiche, religiose o sindacali e a condizione che il trattamento riguardi esclusivamente gli associati o gli ex membri dell'organismo o persone che hanno con esso contatti regolari in relazione alle sue finalità e che i dati personali non siano diffusi all'esterno di tale organismo senza il consenso degli interessati;
(e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
(f) il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o ogni qualvolta i tribunali agiscano in loro capacità;
(g) il trattamento è necessario per motivi di rilevante interesse pubblico, sulla base del diritto dell'Unione o degli Stati membri che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure idonee e specifiche a tutela dei diritti fondamentali e degli interessi dell'interessato;
(h) il trattamento è necessario a fini di medicina preventiva o del lavoro, per la valutazione della capacità lavorativa del dipendente, per la diagnosi medica, per l'erogazione di cure o cure sanitarie o sociali o per la gestione di sistemi e servizi sanitari o sociali sulla base di diritto dell'Unione o dello Stato membro o in virtù di un contratto con un operatore sanitario e soggetti alle condizioni e tutele;
(i) il trattamento è necessario per motivi di interesse pubblico nel settore della salute pubblica, come la protezione contro gravi minacce per la salute a carattere transfrontaliero o la garanzia di standard elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali o dispositivi medici, sulla base dell'Unione o il diritto degli Stati membri che prevede misure idonee e specifiche per salvaguardare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
(j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ai sensi dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o degli Stati membri che è proporzionato allo scopo perseguito, rispetta l'essenza del diritto di protezione dei dati e prevede misure idonee e specifiche a tutela dei diritti fondamentali e degli interessi dell'interessato.

Il consenso

Il **Considerando 32** afferma che il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

L'**Art. 7** stabilisce che, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali e che se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che

riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Inoltre, l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di prestare il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

I Soggetti

Per quanto riguarda i diversi attori che si muovono nello scenario della protezione dei dati, possiamo trovare:

Gli Interessati

Gli interessati sono le persone fisiche, identificate o identificabili, a cui si riferiscono i dati personali.

Titolare - contitolari

In base alla definizione del GDPR il "**titolare del trattamento**" è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; qualora le finalità e i mezzi di tale trattamento siano determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici per la sua nomina possono essere previsti dal diritto dell'Unione o degli Stati membri; qualora due o più titolari del trattamento determinino congiuntamente le finalità e i mezzi del trattamento, sono contitolari del trattamento.

Secondo l'**art. 24** del GDPR, il titolare del trattamento, tenuto conto della natura, dell'ambito, del contesto e delle finalità del trattamento nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, adotta misure tecniche e organizzative adeguate per garantire e poter dimostrare (principio di responsabilità) che il trattamento è svolto in conformità con il Regolamento sulla protezione dei dati. Tali misure sono riesaminate e aggiornate ove necessario.

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari[5] del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli **artt. 13 e 14**, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati ed il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

[5] Si vedano le Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, Versione 2.0 Adottate il 7 luglio 2021 dal EDPB

L'interessato, peraltro, può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento, indipendentemente dalle disposizioni dell'accordo.

I Designati

L'**Art. 2-quaterdecies** del Codice Privacy prevede la possibilità per il titolare, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, di attribuire funzioni e compiti a soggetti designati persone fisiche che operano sotto la loro autorità, ed espressamente designati, affinché svolgano specifici compiti e funzioni connessi al trattamento di dati personali.

L'Agenzia ha adottato con **DDG 117/21** l'atto di designazione in base all'**art. 2-quaterdecies**, prevedendo che i Direttori di Area e i Dirigenti siano Designati nell'ambito delle rispettive attività.

Gli Autorizzati

Il Personale autorizzato al trattamento deve sempre usare la massima discrezione sui dati personali di cui sia a conoscenza, curando attentamente la loro protezione.

Gli Autorizzati possono effettuare il trattamento dei dati personali con conseguente possibilità di

accesso ed utilizzo della documentazione cartacea, degli strumenti informatici, elettronici e telematici, nonché degli archivi/banche dati del titolare del trattamento.

Nell'adempimento delle mansioni assegnate, l'Autorizzato dovrà attenersi alle specifiche istruzioni operative impartite dal Titolare del trattamento, operando con la massima riservatezza e discrezione, accedendo esclusivamente ai Dati la cui conoscenza è strettamente necessaria per adempiere ai compiti assegnatigli ed osservando misure di sicurezza ed istruzioni apposite impartite dal titolare.

Il Responsabile esterno

Il " **responsabile del trattamento** " è una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro organismo che tratta dati personali per conto del responsabile del trattamento.

L'**art. 28** GDPR stabilisce che 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 GDPR e garantisca la tutela dei diritti dell'interessato.

Occorrerà, quindi, che tra titolare e responsabile venga sottoscritto un accordo che abbia i contenuti previsti dall'**art. 28**[6].

[6] 3. 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. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Il DPO

La figura del Data Protection Officer o Responsabile per la Protezione dei Dati personali è prevista dagli **artt. 37-39** del GDPR e, per quanto non sia del tutto nuova, ha di certo comportato un deciso interesse al riguardo[7].

L'**art. 37**, infatti, prevede che Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'**art. 10**.

Il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali e sostenuto nell'esecuzione dei compiti affidati, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Il DPO non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti e non può essere rimosso o penalizzato per l'adempimento dei propri compiti.

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32;
d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Si veda anche la DECISIONE DI ESECUZIONE (UE) 2021/915 DELLA COMMISSIONE Europea del 4 giugno 2021 relativa alle clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento a norma dell'articolo 28, paragrafo 7, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio e dell'articolo 29, paragrafo 7, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio

[7] Si vedano anche le Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016 nonché le FAQ del garante Italiano al seguente indirizzo https://www.garanteprivacy.it/regolamentoue/rpd

Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento ed è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri

Può essere contattato dagli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

Al DPO, anche se può svolgere altri compiti e funzioni che non diano adito a un conflitto di interessi, sono affidati i seguenti compiti (**art. 39**):

o informare e consigliare il titolare del trattamento o il responsabile del trattamento e i dipendenti che svolgono il trattamento dei loro obblighi ai sensi del presente regolamento e di altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati;

o monitorare il rispetto del presente regolamento, delle altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati e delle politiche del titolare o del responsabile del trattamento in relazione alla protezione dei dati personali, compresa l'attribuzione di responsabilità, la sensibilizzazione e la formazione del personale coinvolto nel trattamento operazioni, e le relative verifiche;

o fornire consulenza ove richiesto in merito alla valutazione d'impatto sulla protezione dei dati e monitorarne le prestazioni ai sensi dell'**art. 35**;

o collaborare con l'autorità di controllo;

o fungere da punto di contatto per l'autorità di controllo sulle questioni relative al trattamento, compresa la consultazione preventiva di cui all'**art. 36**, e consultarsi, se del caso, per ogni altra questione.

L'autorità di controllo

Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (**legge 31 dicembre 1996, n. 675**), poi disciplinata dal Codice in materia di protezione dei dati personali (**d.lg. 30 giugno 2003 n. 196 – Codice Privacy**), come modificato dal **Decreto legislativo 10 agosto 2018, n. 101**. Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (**art. 51**).

I Compiti del Garante sono definiti dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101, oltre che da vari altri atti normativi italiani e internazionali.

Il Garante per la protezione dei dati personali si occupa, tra l'altro, di:

- controllare che i trattamenti di dati personali siano conformi al Regolamento nonché a leggi e regolamenti nazionali e prescrivere, ove necessario, ai titolari o ai responsabili dei trattamenti le misure da adottare per svolgere correttamente il trattamento nel rispetto dei diritti e delle libertà fondamentali degli individui;

- collaborare con le altre autorità di controllo e prestare assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del Regolamento;
- esaminare reclami;
- (nel caso di trattamenti che violano le disposizioni del Regolamento) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento e ingiungere di conformare i trattamenti alle disposizioni del Regolamento; imporre una limitazione provvisoria o definitiva del trattamento, incluso il divieto di trattamento; ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento
- adottare i provvedimenti previsti dalla normativa in materia di protezione dei dati personali;
- segnalare, anche di propria iniziativa, al Parlamento e altri organismi e istituzioni l'esigenza di adottare atti normativi e amministrativi relativi alle questioni riguardanti la protezione dei dati personali;
- formulare pareri su proposte di atti normativi e amministrativi;
- partecipare alla discussione su iniziative normative con audizioni presso il Parlamento;
- predisporre una relazione annuale sull'attività svolta e sullo stato di attuazione della normativa sulla privacy da trasmettere al Parlamento e al Governo;
- partecipare alle attività dell'Unione europea ed internazionali di settore, anche in funzione di controllo e assistenza relativamente ai sistemi di informazione Europol, Schengen, VIS, e altri;
- curare l'informazione e sviluppare la consapevolezza del pubblico e dei titolari del trattamento in materia di protezione dei dati personali, con particolare attenzione alla tutela dei minori;
- tenere registri interni delle violazioni più rilevanti e imporre sanzioni pecuniarie ove previsto dal Regolamento e dalla normativa nazionale;
- coinvolgere, ove previsto, i cittadini e tutti i soggetti interessati con consultazioni pubbliche dei cui risultati si tiene conto per la predisposizione di provvedimenti a carattere generale.

SEDE

Piazza Venezia n. 11 - 00187 Roma

www.garanteprivacy.it

Altri soggetti

Tra gli altri soggetti, il GDPR menziona:

- il «**destinatario**», ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento ed

- il «**terzo**», ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Il registro dei trattamenti

Uno degli adempimenti più importanti per il Titolare è istituire e mantenere aggiornato un registro dei trattamenti sotto la propria responsabilità, come previsto dall'**art. 30**.

Tale registro deve contenere tutte le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, inclusi destinatari di paesi terzi o organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione di tale paese terzo o organizzazione internazionale e, nel caso di trasferimenti di cui al secondo comma dell'**art. 49, comma 1**, la documentazione delle garanzie idonee;
- ove possibile, i termini previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'**art. 32**.

L'Agenzia si è dotata di un apposito software - denominato **DPM** (**Data Protection Manager** - raggiungibile all'indirizzo internet **https://aress.privacymanager.eu/login** ed è accessibile con le proprie credenziali) per la gestione degli adempimenti in materia di protezione dei dati personali che contiene anche il registro dei trattamenti.

La DPIA

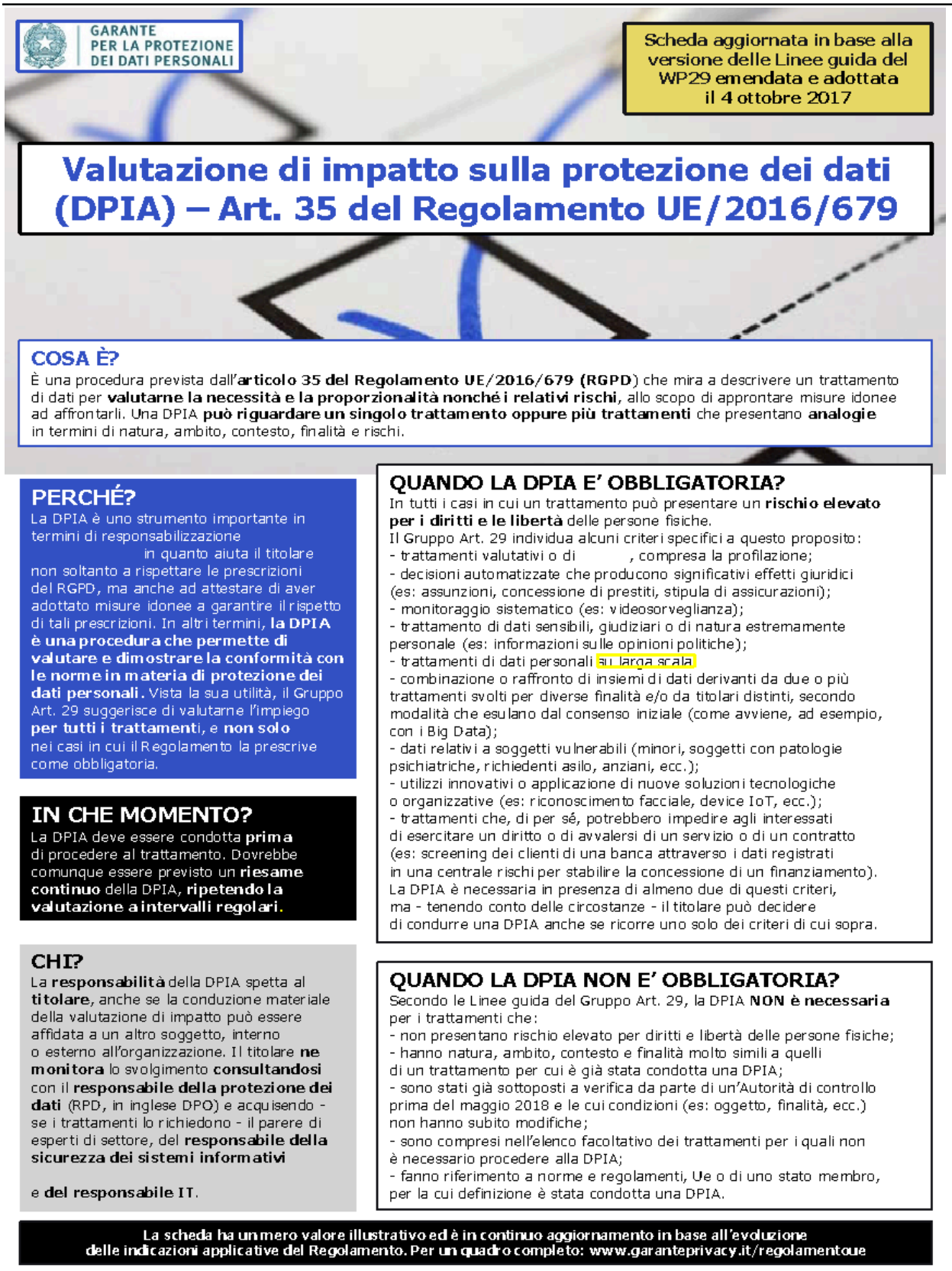
Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono infatti tenuti non soltanto a garantire l'osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Le linee-guida del **WP29**[8] offrono alcuni chiarimenti sul punto; in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all´**art. 35**), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa

[8] Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01

consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGPD)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi**

e **del responsabile IT**.

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di , compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue

Figura 1 - Scheda del Garante per la DPIA

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

*CHIARIMENTO INTERPRETATIVO

ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979]

Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto

(Pubblicato sulla Gazzetta Ufficiale n.

1. Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato"*.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono *"effetti giuridici"* oppure che incidono *"in modo analogo significativamente"* sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Le linee-guida chiariscono, peraltro, anche quando una valutazione di impatto non sia richiesta: ciò vale, in particolare, per i trattamenti in corso che siano già stati autorizzati dalle autorità competenti e non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del regolamento.

Il messaggio finale delle linee-guida è che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l'altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento.

Anche per effettuare la DPIA si può utilizzare il software gestionale **DPM**.

Le misure di sicurezza

Il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento, tenendo 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. Le dette misure debbono essere periodicamente riesaminate e aggiornate.

Infatti, come norma di chiusura, il Regolamento europeo impone l'introduzione anche di una procedura per testare, verificare e valutare, in maniera costante e ciclica, l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento, adeguando o modificando controlli e misure al fine di minimizzare i rischi.

Per tale motivo, il titolare, con cadenza annuale o inferiore in caso di modifiche tecnologiche o di processo produttivo, procede al controllo dell'effettivo funzionamento delle misure di sicurezza organizzative e tecniche poste in essere, provvedendo ai relativi aggiornamenti.

Come indicato dall'**art. 32** Reg. Ue, si possono indicare la pseudonimizzazione e la cifratura dei dati, la capacità di assicurare la riservatezza, la disponibilità e l'integrità su base permanente, anche attraverso la resilienza dei sistemi e dei servizi di trattamento e quella di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

In tale ambito, alla stregua di vera e propria misura di sicurezza, rientra la formazione continua del titolare e del personale.

Per quanto concerne ad esempio la pseudonimizzazione[9], questa deve essere intesa come un particolare trattamento dei dati personali realizzato in modo tale che i dati stessi non possano più essere attribuiti direttamente ed automaticamente ad un interessato specifico.

La cifratura dei dati personali, invece, è quella tecnica più definitiva, volta a rendere i dati personali inintelligibili a chiunque non sia autorizzato ad accedervi e consiste, più specificamente, nella conversione delle informazioni originali in una sequenza apparentemente casuale di numeri, lettere e segni speciali, tale per cui il risultato sia irreversibile attraverso l'utilizzo di meccanismi che normalmente prevedono l'impiego di algoritmi di crittografia.

Ad ogni modo, il Titolare del trattamento mette in atto, anche con l'ausilio dei soggetti esterni che forniscono servizi IT, misure tecniche ed organizzative adeguate per garantire un livello di sicurezza

[9] In tema si veda il report "Pseudonymisation techniques and best practices", pubblicato da Enisa ed il Parere 05/2014 sulle tecniche di anonimizzazione adottato il 10 aprile 2014 dal WP29.

adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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 si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

L'elencazione delle misure contenuta nel GDPR va considerata esemplificativa e non esaustiva e, in questo senso, aperta all'individuazione di altre diverse possibili misure ideate in base al contesto concreto in cui vengono poste in essere.

L'informativa

In esecuzione del principio di trasparenza e per ottemperare in maniera proattiva all'esercizio dei diritti di conoscenza degli interessati, occorre fornire agli utenti ed agli altri interessati l'apposita Informativa, che è un adempimento basilare per qualsiasi titolare previsto dagli **artt. 12, 13 e 14 del GDPR**.

L'informativa richiesta dal Regolamento UE è più ricca di informazioni di quella già prevista nel Codice Privacy: per esempio, il titolare deve esplicitarvi il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo, utilizzando un linguaggio semplice e chiaro, facilmente accessibile, soprattutto se diretta a minori e categorie di interessati vulnerabili, attraverso la pubblicazione sul sito internet e/o la diffusione attraverso supporti cartacei.

Non occorre informare l'interessato quando:

- l'interessato dispone già delle informazioni;
- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare;
- i dati personali debbano rimanere riservati per obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri.

I diritti degli interessati

Il Regolamento europeo disciplina un ampio ventaglio di diritti che spettano all'interessato e dei quali lo stesso deve essere informato.

Si tratta del

1. **diritto di accesso (art. 15)**
2. **diritto di rettifica (art. 16)**
3. **diritto alla cancellazione (più noto come diritto all'oblio) (art. 17)**
4. **diritto di limitazione del trattamento (art. 18)**
5. **diritto alla portabilità dei dati (art. 20)**
6. **diritto di opposizione al trattamento (art. 21)**.

Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento.

Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'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".

Il diritto alla limitazione 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 ai sensi dell´**art. 21** del regolamento (in attesa della valutazione da parte del titolare).

Il diritto alla portabilità, invece, è sicuramente il più innovativo tra i vari diritti. Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico). Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell´interessato o sulla base di un contratto stipulato con l´interessato (quindi non si applica ai dati il cui trattamento si fonda sull´interesse pubblico o sull´interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall´interessato al titolare (si veda il **considerando 68** per maggiori dettagli).

Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste).

La richiesta potrà essere effettuata sul modulo fac-simile predisposto dal Garante Privacy e reperibile sul sito dell'Autorità.

Data breach

Altro importante adempimento è quello relativo alla gestione di eventuali violazioni di dati personali (c.d. data breach) che impongono la tempestiva notifica all'autorità di controllo e se del caso direttamente agli interessati.

Il Regolamento Ue definisce «**violazione dei dati personali**» la violazione di sicurezza che comporta ***accidentalmente*** o ***in modo illecito***

- ✔ la distruzione
- ✔ la perdita
- ✔ la modifica

- ✔ la divulgazione non autorizzata
- ✔ l'accesso ai dati personali

trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Nel caso di una violazione dei dati, il titolare deve comunicare formalmente tale violazione all'Autorità Garante, senza indebito ritardo, e in ogni caso **entro 72 ore** dalla conoscenza.

Il titolare deve tenere un **registro di tutte le violazioni dei dati**, che comprende i fatti e gli effetti della violazione e qualsiasi azione per porvi rimedio.

Tutte le violazioni devono essere registrate (anche quelle piccole e di scarso impatto), e questi dati devono essere comunicati al Garante.

Tuttavia, l'**art. 33** prevede l'esonero da tale notifica nel caso in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

In caso si dovesse verificare una violazione di dati personali, le relative informazioni devono essere comunicate, da chi ha avuto contezza dell'incidente, al Titolare coinvolgendo il Dpo nominato, descrivendo 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, le probabili conseguenze della violazione dei dati personali, le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Occorre, poi, valutare il rischio per le persone derivante dalla violazione (probabilità di: assenza di rischio, a rischio o ad alto rischio) sulla base delle informazioni disponibili relativamente all'incidente di sicurezza, notificando, se del caso, all'autorità di vigilanza ed eventualmente dando comunicazione della violazione alle persone colpite, se necessario.

Il **Considerando 75** del GDPR afferma che i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La documentazione della violazione deve essere fornita man mano che si sviluppa la vicenda. Ogni incidente di sicurezza deve essere riportato nell'apposito registro delle violazioni, anche nel caso in cui non si debba procedere alla notifica al Garante, compilando il modulo rinvenibile sul sito istituzionale dello stesso.

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

L'Agenzia ha predisposto una apposita procedura, approvata con **DDG n. 335/22**, per la gestione di eventuali data breach alla quale si rimanda.

Il trasferimento dei dati all'estero

Il GDPR vieta il trasferimento verso Paesi situati al di fuori dell'UE o organizzazioni internazionali se effettuato in assenza di adeguati standard di tutela. Al contrario, invece, è permesso in caso di presenza di adeguate garanzie come clausole contrattuali tra Titolari autorizzate dal Garante, accordi e provvedimenti vincolanti tra autorità pubbliche amministrative e giudiziarie, clausole tipo adottate dal Garante, adesione a codici di condotta e/o meccanismi di certificazione. È inoltre permesso il trasferimento extra UE in caso di decisioni di adeguatezza della Commissione UE (es. «Privacy Shield EU/USA[10]», Svizzera, Argentina, Australia, Canada, ecc.), norme vincolanti di impresa (Binding Corporate Rules – «BCR») e casi in deroga (consenso informato dell'interessato, necessità per esecuzione adempimenti contrattuali e precontrattuali, interesse pubblico, diritto di difesa, interessi vitali, dati tratti da registro pubblico, ecc.).

[10] Con la sentenza del 16 luglio 2020 relativa alla causa C-311/18, la Corte di Giustizia europea ha dichiarata invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime del Privacy Shield, lo scudo UE-USA per la protezione dei dati personali oggetto di trasferimento verso gli Stati Uniti.

Le sanzioni

L'**art. 82** del GDPR disciplina il diritto al risarcimento e responsabilità in forza del quale chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento.

Il sistema sanzionatorio prevede, a fronte del compimento di violazioni del Regolamento, in funzione delle circostanze di ogni singolo caso, l'applicazione delle seguenti sanzioni amministrative pecuniarie:

- una multa fino a 10 milioni di euro o, se superiore, fino al 2% del volume d'affari globale registrato nell'anno precedente, nei casi previsti dall'**art. 83, paragrafo 4** del Regolamento (a titolo esemplificativo, in caso di: mancata adozione delle tutele per i minori, sui dati anonimizzati, delle misure privacy by design e by default, contitolari, registri del trattamento, privacy impact assessment, istruzioni agli incaricati, misure di sicurezza, data protection officer);

- una multa fino a 20 milioni di euro o, se superiore, fino al 4% del volume d'affari globale registrato nell'anno precedente, nei casi previsti dall'**art. 83, paragrafi 5 e 6** del Regolamento (a titolo esemplificativo, in caso di mancato rispetto dei principi di base del trattamento, dei diritti degli interessati, delle regole sui trasferimenti di dati extra UE, ecc.);

Nell'ambito del GDPR viene stabilito un margine di discrezionalità circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. Ciò non implica un'autonomia gestionale delle sanzioni in capo alle Autorità nazionali competenti, ma fornisce, a queste ultime, alcuni criteri su come interpretare le singole circostanze del caso. I criteri per la determinazione delle sanzioni amministrative pecuniarie (come, a titolo esemplificativo, la natura, gravità e durata della violazione, il carattere doloso o colposo della violazione, il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi) sono stabiliti all'**art. 83 paragrafo 2** del Regolamento.

In sede di adeguamento nazionale alle disposizioni del GDPR, il **D.lgs. 196/2003**, come modificato dal D.lgs. 101/2018, all'**art. 166** ha fornito ulteriori indicazioni in relazione ai criteri di applicazione delle sanzioni amministrative pecuniarie e in relazione al procedimento per l'adozione dei provvedimenti correttivi e sanzionatori.

Secondo quanto stabilito dal **Considerando 149** e dall'**art. 84** del GDPR, l'Italia ha introdotto disposizioni relative a sanzioni penali come strumento di attuazione e tutela della nuova disciplina. In particolare, il **D.lgs. 196/2003**, come modificato dal D.lgs. 101/2018, ha previsto specifiche fattispecie penali agli **artt. 167, 167 bis, 167 ter, 168, 170 e 171**.

Secondo l'**art. 58** del GDPR, le Autorità possono avvalersi inoltre di una serie di poteri correttivi come la possibilità di limitare o addirittura vietare un trattamento dei dati da parte del titolare.

La direttiva e-privacy e i cookies

Oltre al regolamento generale, dovrebbe essere preso in considerazione un altro atto normativo. Si tratta della cosiddetta **Direttiva ePrivacy**, il cui **art. 5** prevede che l'archiviazione di informazioni sul dispositivo dell'utente o l'accesso alle informazioni già archiviate è consentito solo se

(i) l'utente ha prestato il consenso

(ii) o la memorizzazione e/o l'accesso è strettamente necessario per il servizio della società dell'informazione (es. l'app) esplicitamente richiesto (cioè installato e attivato) dall'utente.

Detta direttiva è molto importante perché costituisce il riferimento normativo per un tema molto conosciuto con il nome di **cookies**.

1.2 Quadro italiano

L'Italia, a seguito dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati (Regolamento (UE) 2016/679) (GDPR), ha dovuto modificare il Codice della Privacy (D.lgs. n. 196/2003), che contiene disposizioni per adeguare la normativa nazionale al Regolamento Generale sulla Protezione dei Dati (Regolamento (UE) 2016/679) e che abroga sezioni direttamente in contrasto con il GDPR. Questo è stato un passo dovuto in considerazione del fatto che le disposizioni contenute nel GDPR sono preminenti rispetto a quelle interne, e queste sarebbero state implicitamente abrogate, creando potenziali fraintendimenti interpretativi. L'attività di modifica è stata svolta dal **Decreto Legislativo 10 agosto 2018 n. 101**, che ha modificato il testo del **Decreto Legislativo n. 196/2003 (Codice Privacy)** al fine di adeguarlo al GDPR.

Il controllo sull'applicazione del Regolamento è svolto dal Garante per la protezione dei dati personali italiano ("Garante"), che, tra l'altro, riceve i reclami degli interessati, prevede specifiche misure di protezione dei dati per i titolari e responsabili del trattamento e adotta linee guida per assistere organizzazioni nel rispetto del GDPR.

Una delle disposizioni più importanti del regolamento interno è l'**art. 2-ter del Codice Privacy**, il quale prevede che i dati personali possono essere comunicati tra titolari del trattamento per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri solo se:

- ✔ ciò è previsto da una legge
- ✔ oppure, ove previsto da una legge o da un regolamento; ovvero ciò sia necessario per l'espletamento di compiti di interesse pubblico o per l'adempimento di doveri istituzionali e il Garante ne sia stato preventivamente informato.

Inoltre, ai sensi dell'**art. 2-ter, 1-bis del Codice Privacy**, introdotto dall'**art. 9** del **decreto legge 8 ottobre 2021, n. 139**, le pubbliche amministrazioni, le autorità indipendenti, nonché le società a controllo pubblico sono sempre autorizzate a trattare i dati personali se necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri allo stesso conferiti. Ove la finalità del trattamento non sia prevista né da una legge né da un regolamento, la finalità del trattamento è indicata dalla stessa amministrazione/società a controllo statale in linea con il compito svolto o i poteri esercitati. Si precisa che tale disposizione si applica ai soli dati personali generici e non a categorie particolari.

Trattamento necessario per motivi rilevanti di interesse pubblico

L'**Art. 2-sexies del Codice Privacy**, che affronta le eccezioni previste dall'**art. 9, comma 1, lettera g), GDPR**, prevede che il trattamento di categorie particolari di dati personali per motivi di rilevante interesse pubblico

sia effettuato solo se attinenti entrambi le aree indicate nell'**art. 2-sexies del Codice Privacy** ed è previsto dalla normativa comunitaria o italiana o, ove previsto dalla legge, da regolamenti.

Detto articolo prevede che i trattamenti delle categorie particolari di dati personali di cui all'**art. 9, paragrafo 1**, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del **paragrafo 2, lettera g)**, del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Fermo quanto appena detto e previsto dal **comma 1**, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

a) accesso a documenti amministrativi e accesso civico;
b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
c) tenuta di registri pubblici relativi a beni immobili o mobili;
d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;
h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;
i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale, comprese quelle di prevenzione e contrasto all'evasione fiscale;
j) attività di controllo e ispettive;
k) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;
l) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;
m) rapporti tra i soggetti pubblici e gli enti del terzo settore;

n) obiezione di coscienza;
o) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;
p) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;
q) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;
r) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;
s) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;
t) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;
u) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
v) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;
w) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;
x) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);
y) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

Elaborazione dei dati sanitari per finalità di ricerca medica, biomedica ed epidemiologica

L'**Art. 110 del Codice Privacy** consente il trattamento dei dati sanitari in ambito medico, biomedico ed epidemiologico senza il consenso dell'interessato per l'archiviazione nel pubblico interesse, di ricerca scientifica o storica. Tale trattamento è consentito se la normativa comunitaria o italiana o, ove previsto da una legge, un regolamento autorizza la ricerca scientifica e il titolare effettua una DPIA che viene messa a disposizione del pubblico, o se l'informazione degli interessati comporta uno sforzo sproporzionato o è idonea a rendere impossibile o pregiudicare gravemente il raggiungimento degli scopi di ricerca (alle condizioni previste dal Codice). Infine, l'**art. 110, comma 2, del Codice** prevede che i titolari del trattamento in tali circostanze che ricevono una richiesta di rettifica o di completamento dell'interessato ai sensi dell'**art. 16** GDPR devono registrare la richiesta senza modificare i dati se i dati rettificati o completati non producono effetti significativi sull'esito della ricerca.

Elaborazione di dati genetici, biometrici e sanitari

L'**art. 2-septies del Codice** prevede che il trattamento dei dati genetici, biometrici e sanitari sia effettuato solo se il trattamento è conforme sia all'**art 9, comma 2, GDPR** sia ad alcune misure di sicurezza (quali crittografia, pseudonimizzazione e minimizzazione) sono implementati. Tali misure di sicurezza saranno stabilite dal "Garante" con cadenza almeno biennale. Tuttavia, finora l'autorità italiana non ha adottato nuove tutele da quando è entrato in vigore il GDPR.

Trattamento di dati personali in ambito sanitario

Il **Titolo V del Codice privacy** disciplina il trattamento di dati personali in ambito sanitario.

L'**Art. 75** disciplina le specifiche condizioni in ambito sanitario prevedendo che il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'**art. 9, paragrafi 2, lettere h) ed i), e 3** del regolamento, dell'**art. 2-septies del presente codice**, nonché nel rispetto delle specifiche disposizioni di settore.

Infatti, l'**Art. 77** permette alle strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie ed agli esercenti le professioni sanitarie di poter adottare modalità particolari per informare l'interessato ai sensi degli **artt. 13 e 14** del Regolamento e per il trattamento dei dati personali.

In particolare, Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati negli **artt. 13 e 14** del Regolamento.

Le informazioni possono essere fornite per il complessivo trattamento dei dati personali necessario per attività di diagnosi, assistenza e terapia sanitaria, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

Le informazioni possono riguardare, altresì, dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto.

Le informazioni, se non è diversamente specificato dal medico o dal pediatra, riguardano anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

a) sostituisce temporaneamente il medico o il pediatra;
b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;
c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;
d) fornisce farmaci prescritti;
e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

Le informazioni rese evidenziano analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;
b) nell'ambito della teleassistenza o telemedicina;
c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica;

c-bis) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'**art. 12 del decreto-legge 18 ottobre 2012, n. 179**, convertito, con modificazioni, dalla **legge 17 dicembre 2012, n. 221**;

c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'**art. 12 del decreto-legge 18 ottobre 2012, n. 179**, convertito, con modificazioni, dalla **legge 17 dicembre 2012, n. 221**.

L'**art. 79** consente alle strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie di avvalersi delle modalità particolari in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate, permettendo di annotare l'avvenuta informazione con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

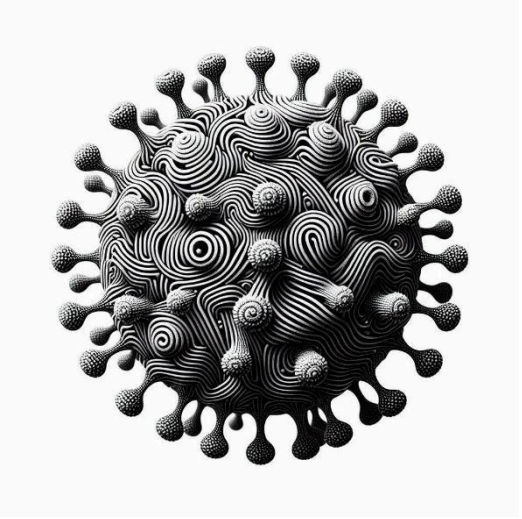
In base all'**Art. 92**, nei casi in cui strutture, pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'**art. 9, paragrafo 2, lettera f)**, del Regolamento, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale
b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

Periodo pandemico

In questo contesto, la pandemia di Covid-19 ha creato sfide senza precedenti per l'Unione e gli Stati membri, i loro sistemi sanitari, il loro stile di vita, la stabilità economica e i loro valori. Le tecnologie e i dati digitali hanno un ruolo prezioso da svolgere nella lotta alla crisi del COVID-19. Le applicazioni mobili tipicamente installate su smartphone (app) possono supportare le autorità sanitarie pubbliche a livello nazionale e dell'UE nel monitoraggio e nel contenimento della pandemia di COVID-19 e sono particolarmente rilevanti nella fase di sollevamento delle misure di contenimento.



Infatti, poiché il mondo sta affrontando una grave crisi di salute pubblica che richiede risposte forti, che, come stiamo effettivamente vivendo, hanno un impatto oltre l'emergenza, l'elaborazione automatizzata dei dati e le tecnologie digitali possono essere componenti chiave nella lotta al COVID-19.

I governi e gli attori privati si stanno orientando verso l'uso di soluzioni basate sui dati come parte della risposta alla pandemia di COVID-19, sollevando numerosi problemi di privacy.

Ad ogni modo, il quadro giuridico sulla protezione dei dati è stato concepito per essere flessibile e, in quanto tale, è in grado di ottenere sia una risposta efficiente nel limitare la pandemia, sia proteggere i diritti umani e le libertà fondamentali.

Le norme in materia di protezione dei dati (come il GDPR), infatti, non ostacolano le misure adottate nella lotta alla pandemia di COVID - 19, perché il GDPR è un atto legislativo ampio e prevede diverse disposizioni che consentono di gestire il trattamento dei dati personali dati per finalità di ricerca scientifica connessa alla pandemia di COVID-19 nel rispetto dei diritti fondamentali alla privacy e alla protezione dei dati personali. Il GDPR prevede anche una specifica deroga al divieto di trattamento di alcune categorie particolari di dati personali, come i dati sanitari.

Quando il trattamento dei dati personali è necessario per gestire la pandemia di COVID-19, la protezione dei dati è indispensabile per creare fiducia, creare le condizioni per l'accettabilità sociale di qualsiasi soluzione e quindi garantire l'efficacia di queste misure.

L'identificazione di chi decide i mezzi e le finalità del trattamento dei dati (il titolare del trattamento) è fondamentale per stabilire chi è responsabile del rispetto delle norme dell'UE in materia di protezione dei dati personali, e in particolare: chi dovrebbe fornire informazioni alle persone fisiche, chi scarica l'app su cosa accadrà con i propri dati personali (già esistenti o da generare tramite il dispositivo, ad esempio uno smartphone, su cui è installata l'app), quali saranno i suoi diritti, chi sarà responsabile in caso di violazione dei dati, ecc.

Data la sensibilità dei dati personali in questione e le finalità del trattamento dei dati descritte di seguito, la Commissione ritiene che le app debbano essere progettate in modo tale che le autorità sanitarie nazionali (o gli enti che svolgono compiti di interesse pubblico nel campo della salute) siano i responsabili del trattamento. I titolari del trattamento sono responsabili del rispetto del GDPR (principio di accountability).

Un fattore determinante per la fiducia delle persone nelle app è dimostrare che mantengono il controllo dei propri dati personali. Per garantire ciò, la Commissione ritiene che in particolare dovrebbero essere soddisfatte le seguenti condizioni:

- L'installazione dell'app sul proprio dispositivo deve essere volontaria e senza conseguenze negative per il soggetto che decide di non scaricare/utilizzare l'app;

- le autorità sanitarie dovrebbero fornire alle persone tutte le informazioni necessarie relative al trattamento dei loro dati personali (in linea con gli **artt. 12 e 13** del GDPR e l'**art. 5 della Direttiva ePrivacy**);
- l'individuo dovrebbe poter esercitare i propri diritti ai sensi del GDPR (in particolare, accesso, rettifica; cancellazione). Qualsiasi restrizione dei diritti ai sensi del GDPR e della Direttiva ePrivacy dovrebbe essere conforme a tali atti ed essere necessaria, proporzionata e prevista dalla legislazione;
- le app dovrebbero essere disattivate al più tardi quando la pandemia sarà dichiarata sotto controllo; la disattivazione non dovrebbe dipendere dalla disinstallazione da parte dell'utente.

Come detto sopra, tutti i trattamenti di dati personali concernenti la salute devono essere conformi ai principi relativi al trattamento di cui all'**art. 5** GDPR e ad una delle basi giuridiche e delle specifiche deroghe elencate rispettivamente all'**art. 6** e all'**art. 9** GDPR per il trattamento lecito di questa categoria speciale di dati personali.

Secondo **EDPB**, il consenso dell'interessato, raccolto ai sensi dell'**art. 6, paragrafo 1, lettera a)** e dell'**art. 9, paragrafo 2, lettera a)**, del GDPR, può costituire una base giuridica per il trattamento dei dati relativi alla salute nell'emergenza COVID-19. Tuttavia, si precisa che devono essere soddisfatte tutte le condizioni per il consenso esplicito, in particolare quelle di cui all'**art 4, paragrafo 11**, all'**art. 6, paragrafo 1, lettera a)**, all'**art. 7** e all'**art. 9, paragrafo 2, lettera a)**, del GDPR. In particolare, il consenso deve essere dato liberamente, specifico, informato e inequivocabile e deve essere espresso mediante una dichiarazione o una "chiara azione affermativa". Come affermato al **considerando 43**, il consenso non può considerarsi liberamente prestato in presenza di un evidente squilibrio tra l'interessato e il titolare del trattamento. È quindi importante che un interessato non subisca pressioni e non subisca svantaggi se decide di non prestare il consenso.

Durante la pandemia, il **Decreto Legge n.18/20**, convertito nella **Legge n. 27/20**, è stato emanato per far fronte a specifiche esigenze nel trattamento della protezione dei dati. Il suo **art. 17-bis** recita:

1. Fino al termine dello stato di emergenza deciso dal Consiglio dei ministri in data 31 gennaio 2020, per motivi di interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la tutela dall'emergenza sanitaria di natura transfrontaliera causata dalla diffusione del COVID-19 mediante adeguate misure di profilassi e per garantire la diagnosi e l'assistenza sanitaria dei contagiati o la gestione dell'emergenza del Servizio Sanitario Nazionale, ai sensi dell'articolo 9, comma 2, lettere g), h) e (i) e dell'articolo 10 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e dell'articolo 2-sexies, comma 2, lettere t) e (u), del Codice di cui al decreto legislativo no. 196 del 30 giugno 2003. 196, i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del codice di cui al decreto legislativo 2 gennaio 2018, n. 1, e gli organi esecutivi di cui all'articolo 1 dell'Ordinanza del Capo del Dipartimento della Protezione Civile n. 630 del 3 febbraio 2020, nonché gli uffici del Ministero della Salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private operanti nell'ambito del Servizio Sanitario Nazionale e gli enti preposti al controllo e alla vigilanza sull'esecuzione delle misure disposte ai sensi dell'art. 2 del decreto-legge n. 25 marzo 2020, n. 19, anche al fine di assicurare la più efficace gestione dei flussi e degli interscambio di dati personali, può effettuare il trattamento, compresa la comunicazione tra gli stessi, di dati personali, anche in relazione agli articoli 9 e 10 del Regolamento (UE) 2016/679, che sono necessari per lo

svolgimento delle funzioni loro assegnate nell'ambito dell'emergenza causata dalla diffusione del COVID-19.

2. La comunicazione di dati personali a soggetti pubblici e privati, diversi da quelli di cui al comma 1, nonché la diffusione di dati personali diversi da quelli di cui agli articoli 9 e 10 del citato Regolamento (UE) 2016/679, essere effettuati nei casi in cui siano indispensabili per lo svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in corso.
3. Il trattamento dei dati personali di cui ai commi 1 e 2 è effettuato nel rispetto dei principi di cui all'articolo 5 del citato Regolamento (UE) 2016/679, adottando misure idonee a tutelare i diritti e le libertà degli interessati.
4. Vista la necessità di conciliare le esigenze di gestione dell'emergenza sanitaria in corso con la necessità di tutelare la riservatezza degli interessati, i soggetti di cui al comma 1 possono rilasciare le autorizzazioni di cui all'articolo 2-quaterdecies del codice di cui alla nel Decreto Legislativo n. 196 del 30 giugno 2003, in via semplificata, anche verbalmente.
5. Nell'attuale contesto emergenziale, ai sensi dell'articolo 23, comma 1, lettera e) del citato Regolamento (UE) 2016/679, fermo restando quanto previsto dall'articolo 82 del codice di cui al decreto legislativo n. 196 del 30 giugno 2003, i soggetti di cui al comma 1 del presente articolo possono omettere le informazioni di cui all'articolo 13 del medesimo Regolamento o fornire informazioni semplificate, previa comunicazione orale agli interessati dalla limitazione.
6. Al termine dello stato di emergenza di cui alla delibera del Consiglio dei ministri del 31 gennaio 2020, i soggetti di cui al comma 1 adottano misure idonee a far rientrare il trattamento dei dati personali effettuato nell'ambito dell'emergenza l'ambito delle competenze ordinarie e la disciplina in materia di trattamento dei dati personali.

Già il codice privacy con l'**Art. 82** disciplina le emergenze e tutela della salute e dell'incolumità fisica prevedendo che le informazioni di cui agli **artt. 13 e 14** del Regolamento possono essere rese senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'**art. 117** del **decreto legislativo 31 marzo 1998, n. 112**.

Tali informazioni possono altresì essere rese senza ritardo, successivamente alla prestazione, in caso di:

a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'**art. 4 della legge 22 dicembre 2017, n. 219** o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato;
b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato.

Le informazioni possono essere rese senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che può essere pregiudicata dal loro preventivo rilascio, in termini di tempestività o efficacia.

Infine, dopo il raggiungimento della maggiore età le informazioni sono fornite all'interessato nel caso in cui non siano state fornite in precedenza.

Linee guida per la pubblicazione dei documenti in Amministrazione Trasparente

La sezione "Amministrazione Trasparente", introdotta con il **D. Lgs. 33/2013** (successivamente modificato dal **D.Lgs. 97/ 2016, c.d. FOIA**), prevede la pubblicazione obbligatoria online sul sito web istituzionale di alcune informazioni relative all'amministrazione e al suo operato in ossequio al principio di trasparenza, intesa come "accessibilità totale", ovvero favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.

Principi generali

Accuratezza e Aggiornamento: Pubblicare solo dati esatti, aggiornati e contestualizzati.

Necessità: Pubblicare solo i dati la cui pubblicazione è realmente necessaria per finalità di trasparenza.

Rispetto della Privacy: Evitare la pubblicazione di dati sensibili come quelli relativi alla salute, alla vita sessuale, all'etnia, alla religione e alle appartenenze politiche, salvo nei casi strettamente indispensabili.

Tipologie di Atti da Pubblicare

Provvedimenti Amministrativi: Pubblicare gli elenchi dei provvedimenti finali adottati dagli organi di indirizzo politico e dai dirigenti.

Accordi e Convenzioni: Pubblicare gli accordi stipulati con soggetti privati o altre amministrazioni pubbliche, inclusi protocolli d'intesa e convenzioni.

Modalità di Pubblicazione

Formato Aperto: I dati devono essere pubblicati in formato aperto, ma non necessariamente come "dati aperti" liberamente utilizzabili da chiunque.

Anonimizzazione: Prima di pubblicare dati personali, procedere alla loro anonimizzazione per evitare l'identificazione diretta o indiretta degli interessati.

Indicizzazione: Adottare misure per impedire l'indicizzazione dei dati sensibili da parte dei motori di ricerca.

Durata della pubblicazione

I documenti pubblicati in amministrazione trasparente devono restare online per una durata di **5 anni**, **decorrenti dal 1° gennaio dell'anno successivo** a quello da cui decorre l'obbligo di pubblicazione, salve diverse tempistiche dettate dalla norma per talune informazioni specifiche (**delibera ANAC del 19 dicembre 2023, n. 601**, che aggiorna e integra la **delibera ANAC del 20 giugno 2023, n. 264**). Dopo i predetti termini, la trasparenza è assicurata mediante la possibilità di presentare l'istanza di accesso civico ai sensi dell'**art. 5**

delle **linee guida ANAC (Delibera 1310/2016)** recanti indicazioni "Sull'attuazione degli obblighi di Pubblicità, Trasparenza e diffusione di informazioni contenute nel D.Lgs. 33/2013 come modificato dal D.Lgs. 97/2016".

Sono tuttavia espressamente previste **deroghe** alla predetta durata temporale quinquennale, quale periodo di mantenimento dei dati, informazioni e documenti sul web e cioè, come indicato a **pag.26 delle Linee Guida del Garante (Provvedimento n. 243 del 15 maggio 2014)**:

a) nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;
b) per alcuni dati e informazioni riguardanti i "titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale" (**art. 14, comma 2**) e i "titolari di incarichi dirigenziali e di collaborazione o consulenza" che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico (**art. 15, comma 4**);
c) nel caso in cui siano previsti "diversi termini" dalla normativa in materia di trattamento dei dati personali. In merito, si evidenzia come il Codice – che non prevede termini espliciti (come già evidenziato dal Garante nel **parere del 7 febbraio 2013 (32)**), – richiede espressamente che i dati personali devono essere "conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati" e che l'interessato ha diritto di ottenere la cancellazione dei dati personali "di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati" (**artt. 11, comma 1, lett. e, e 7, comma 3, lett. b, del Codice**).

Inoltre si evidenzia che in applicazione del principio del primato del diritto europeo, il diritto nazionale deve essere interpretato in maniera conforme al diritto europeo e, nello specifico, alle disposizioni direttamente applicabili che impongono il rispetto dei principi di pertinenza, necessità e proporzionalità, in base alle quali la pubblicazione dei dati personali è consentita soltanto quando è al contempo necessaria e appropriata rispetto all'obiettivo perseguito e, in particolare, quando l'obiettivo perseguito non può essere realizzato in modo ugualmente efficace con modalità meno pregiudizievoli per la riservatezza degli interessati. Per tale motivo il Garante ritiene che laddove atti, documenti e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere oscurati, anche prima del termine di cinque anni, quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti stessi hanno prodotto i loro effetti.

Nello specifico si riporta la durata di pubblicazione per ciascuna tipologia di atto:

1. Provvedimenti Amministrativi
Durata: 5 anni dalla data di pubblicazione.

Eccezioni: Se il provvedimento riguarda dati sensibili o giudiziari, la durata può essere ridotta a 3 anni, previa anonimizzazione dei dati personali.

2. Accordi e Convenzioni
Durata: 5 anni dalla data di stipula.

Eccezioni: Gli accordi che contengono dati sensibili o strategici possono essere pubblicati per un periodo ridotto di 3 anni, con eventuale anonimizzazione.

3. Bandi di Gara e Contratti

Durata: 5 anni dalla data di aggiudicazione.

Eccezioni: I dati relativi ai partecipanti non aggiudicatari possono essere rimossi dopo 1 anno, mantenendo solo i dati dell'aggiudicatario.

4. Bilanci e Rendiconti

Durata: 10 anni dalla data di approvazione.

Eccezioni: Nessuna eccezione specifica, ma è possibile rimuovere i dati personali non necessari dopo 5 anni.

5. Delibere e Determine

Durata: 5 anni dalla data di pubblicazione.

Eccezioni: Le delibere contenenti dati sensibili possono essere pubblicate per un periodo ridotto di 3 anni, previa anonimizzazione.

6. Atti di Concessione

Durata: 5 anni dalla data di concessione.

Eccezioni: Gli atti che contengono dati personali sensibili possono essere pubblicati per un periodo ridotto di 3 anni, previa anonimizzazione.

7. Dati e documenti dei titolari di incarichi di collaborazione o consulenza

Devono essere pubblicati entro tre mesi dal conferimento dell'incarico e per i tre anni successivi alla cessazione dell'incarico.

8. Dati dei componenti dell'Organismo Indipendente di Valutazione (OIV)

Devono essere conservati per i tre anni successivi alla cessazione dell'incarico.

Accesso Civico

Accesso Semplice: Garantire l'accesso civico semplice ai dati pubblicati, permettendo ai cittadini di richiedere informazioni non presenti sul sito.

Accesso Generalizzato: Consentire l'accesso civico generalizzato per favorire la partecipazione e il controllo da parte dei cittadini.

Dati non pubblicabili

È necessario sempre valutare attentamente la necessità e la proporzionalità della pubblicazione dei dati personali, oscurando o anonimizzando le informazioni quando possibile per rispettare i diritti e le libertà fondamentali degli individui.

1. Dati Personali Sensibili

Non possono essere pubblicati dati e Informazioni che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona.

- *Riferimento Normativo: Art. 9 del GDPR (https://www.garanteprivacyitalia.it/wp-content/uploads/Circolare-GPI-del-21-aprile-2021-Linee-Guida-per-la-Pubblicazione-dei-Dati-On-Line_Vers.01-Rev.-01-1.pdf).*

2. Dati Personali Comuni

Possono essere pubblicati solo se strettamente necessari per finalità di trasparenza e se previsti da una norma di legge o regolamento.

- *Riferimento Normativo: Art. 6 del GDPR (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3152130).*

3. Dati giudiziari

Non possono essere pubblicate informazioni relative a condanne penali e reati o a misure di sicurezza connesse.

- *Riferimento: https://www.anticorruzione.it/-/trasparenza-e-tutela-dei-dati-personali-modalit%C3%A0-di-pubblicazione-dei-dati-e-limite-della-riservatezza-art.-7-bis-d.lgs.-33/2013-*

4. Dati economici e patrimoniali

Dettagli specifici sulle condizioni economiche e patrimoniali che potrebbero causare imbarazzo o danno all'individuo, come informazioni su debiti o situazioni finanziarie difficili.

- *Riferimento: https://www.garanteprivacyitalia.it/wp-content/uploads/Circolare-GPI-del-21-aprile-2021-Linee-Guida-per-la-Pubblicazione-dei-Dati-On-Line_Vers.01-Rev.-01-1.pdf*

5. Dati relativi a minori

Qualsiasi informazione che possa identificare direttamente o indirettamente un minore.

- *Riferimento: https://www.garanteprivacyitalia.it/wp-content/uploads/Circolare-GPI-del-21-aprile-2021-Linee-Guida-per-la-Pubblicazione-dei-Dati-On-Line_Vers.01-Rev.-01-1.pdf*

6. Dati non pertinenti

Informazioni che non sono strettamente necessarie per le finalità di trasparenza e che non hanno una base giuridica per la pubblicazione

- *Riferimento: https://www.anticorruzione.it/-/trasparenza-e-tutela-dei-dati-personali-modalit%C3%A0-di-pubblicazione-dei-dati-e-limite-della-riservatezza-art.-7-bis-d.lgs.-33/2013-*

7. Dati Anonimizzati

Possono essere pubblicati senza restrizioni, purché l'anonimizzazione sia tale da non permettere l'identificazione, anche indiretta, degli interessati.

- *Riferimento Normativo: Considerando 26 del GDPR (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1793203).*

8. Curricula Professionali

Possono essere pubblicati i curricula dei dirigenti e dei titolari di incarichi dirigenziali, ma devono essere omessi i dati sensibili (codice fiscale, indirizzi, numeri di telefono, email, fotografie…).

- *Riferimento Normativo: D.Lgs. 33/2013, Art. 15 (https://www.anticorruzione.it/-/trasparenza-e-tutela-dei-dati-personali-modalit%C3%A0-di-pubblicazione-dei-dati-e-limite-della-riservatezza-art.-7-bis-d.lgs.-33/2013-).*

9. Compensi e Rimborsi

Possono essere pubblicati i dati relativi ai compensi, ai rimborsi e ai dati patrimoniali dei dirigenti e dei titolari di incarichi dirigenziali.

- *Riferimento Normativo: D.Lgs. 33/2013, Art. 14 (https://www.anticorruzione.it/-/trasparenza-e-tutela-dei-dati-personali-modalit%C3%A0-di-pubblicazione-dei-dati-e-limite-della-riservatezza-art.-7-bis-d.lgs.-33/2013-).*

10. Bandi di Gara e Contratti

Possono essere pubblicati i dati relativi ai bandi di gara e ai contratti, ma devono essere omessi i dati personali non necessari.

- *Riferimento Normativo: D.Lgs. 33/2013, Art. 37 (https://www.anticorruzione.it/-/trasparenza-e-tutela-dei-dati-personali-modalit%C3%A0-di-pubblicazione-dei-dati-e-limite-della-riservatezza-art.-7-bis-d.lgs.-33/2013-).*

11. bandi di concorso

"con particolare riferimento ai provvedimenti finali adottati all'esito dell'espletamento di concorsi oppure di prove selettive non devono formare quindi oggetto di pubblicazione, in base alla disposizione in esame, gli atti nella loro veste integrale contenenti (anche in allegato), le graduatorie formate a conclusione del procedimento, né le informazioni comunque concernenti eventuali prove intermedie che preludono all'adozione dei provvedimenti finali" (Linee guida del Garante predisposte in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"(**provv.n.243 del 15 maggio 2014, doc web n.3134436) pagg.32 e 44**).

12. Elenchi dei Provvedimenti

Possono essere pubblicati gli elenchi dei provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti, omettendo i dati personali non necessari.

- *Riferimento Normativo: D.Lgs. 33/2013, Art. 23 (https://www.anticorruzione.it/-/trasparenza-e-tutela-dei-dati-personali-modalit%C3%A0-di-pubblicazione-dei-dati-e-limite-della-riservatezza-art.-7-bis-d.lgs.-33/2013-).*

13. Registro degli Accessi

Può essere pubblicato il registro degli accessi, ma devono essere omessi i dati personali non necessari.

- *Riferimento Normativo: D.Lgs. 33/2013, Art. 5 (https://www.anticorruzione.it/-/trasparenza-e-tutela-dei-dati-personali-modalit%C3%A0-di-pubblicazione-dei-dati-e-limite-della-riservatezza-art.-7-bis-d.lgs.-33/2013-).*

14. Accorgimenti Tecnici

Devono essere adottati accorgimenti tecnici per impedire l'indicizzazione dei dati personali da parte dei motori di ricerca.

Riferimento Normativo: Linee guida del Garante Privacy (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3152130).

Linee guida per la pubblicazione dei documenti in albo pretorio

L'albo pretorio è una sezione apposita del sito istituzionale, dove vengono pubblicati avvisi ed atti di interesse pubblico.

Il contenuto degli atti da pubblicare è molto ampio e comprende delibere, determine, ordinanze ed altri provvedimenti che per legge devono essere portati a conoscenza del pubblico o di determinate categorie di soggetti interessati.

In alcuni casi, questa forma di pubblicità ha valore legale, come per gli avvisi rivolti ai contribuenti, le pubblicazioni di matrimonio o le informazioni sull'irreperibilità di alcuni cittadini destinatari di provvedimenti amministrativi e giudiziari.

I dati pubblicati nell'albo pretorio devono rimanere visibili per un **periodo di tempo non inferiore a 15 giorni consecutivi** (*https://www.garanteprivacyitalia.it/wp-content/uploads/VADEMECUM-BREVE_Albo-Pretorio-e-pubblicazioni.pdf*). Questo periodo può variare in base alla normativa specifica o alle esigenze del procedimento amministrativo, ma 15 giorni è il termine minimo generalmente previsto.

Dopo la scadenza del periodo di pubblicazione, i documenti vengono archiviati e non sono più visibili al pubblico, ma restano disponibili per eventuali consultazioni interne.

Un caso pilota

Il Garante per la privacy prima e la Cassazione poi (Cass. Sez. 2° Civile, sent. n. 18292/20 del 3 settembre 2020) hanno sanzionato un Ente locale per aver tenuto sull'albo online i dati personali di un dipendente per un periodo eccedente i 15 giorni stabiliti dalla legge.

La sentenza della Suprema Corte specifica che «il Comune è stato sanzionato non per aver pubblicato sul proprio sito le determinazioni dirigenziali, ma per aver mantenuto la pubblicazione oltre il termine di 15 giorni previsto dall'art.124 del Tuel». Infatti «la pubblicazione non poteva ritenersi consentita per un tempo eccedente i 15 giorni in quanto riguardava notizie relative alla vita privata dell'impiegata (il suo stato di famiglia, il fatto di vivere da sola, la proposizione di domanda di rateizzazione, il mancato accoglimento della stessa)».

Questo tipo di informazioni esulava completamente dalle condizioni di trasparenza, dunque la loro pubblicazione non poteva ritenersi legittimata, come hanno rilevato dapprima il Garante per la privacy, che ha sanzionato il Comune al pagamento della somma di 4.000 euro, e successivamente la Corte di Cassazione che ha confermato il provvedimento, respingendo il ricorso dell'Ente avverso la sanzione irrogata.

In alcune situazioni specifiche i documenti possono rimanere pubblicati per **un periodo superiore ai 15 giorni**:

Atti di particolare rilevanza:
Alcuni atti (ad esempio quelli relativi a piani urbanistici o regolamenti comunali), possono richiedere un periodo di pubblicazione più lungo per garantire una maggiore trasparenza e partecipazione pubblica.

Procedimenti amministrativi complessi:
In casi di procedimenti amministrativi che richiedono un'ampia consultazione pubblica o che coinvolgono più enti, il periodo di pubblicazione può essere esteso oltre i 15 giorni per consentire a tutti gli interessati di prendere visione dei documenti.

Normative specifiche:
Alcune normative regionali o locali possono prevedere periodi di pubblicazione più lunghi per determinati tipi di atti o documenti.

Richieste di proroga:
In alcuni casi, può essere richiesta una proroga del periodo di pubblicazione per motivi specifici, come la necessità di ulteriori verifiche o approfondimenti.

È importante che ogni estensione del periodo di pubblicazione sia giustificata e conforme alle normative vigenti per garantire la trasparenza e la legalità del procedimento amministrativo.

Linee guida del Garante Privacy per la pubblicazione dei dati online

Altri riferimenti sulla pubblicazione dei dati online possono essere rivenuti dalle linee guida del Garante pubblicate il 21 aprile 2021 (https://www.garanteprivacyitalia.it/wp-content/uploads/Circolare-GPI-del-21-aprile-2021-Linee-Guida-per-la-Pubblicazione-dei-Dati-On-Line_Vers.01-Rev.-01-1.pdf)