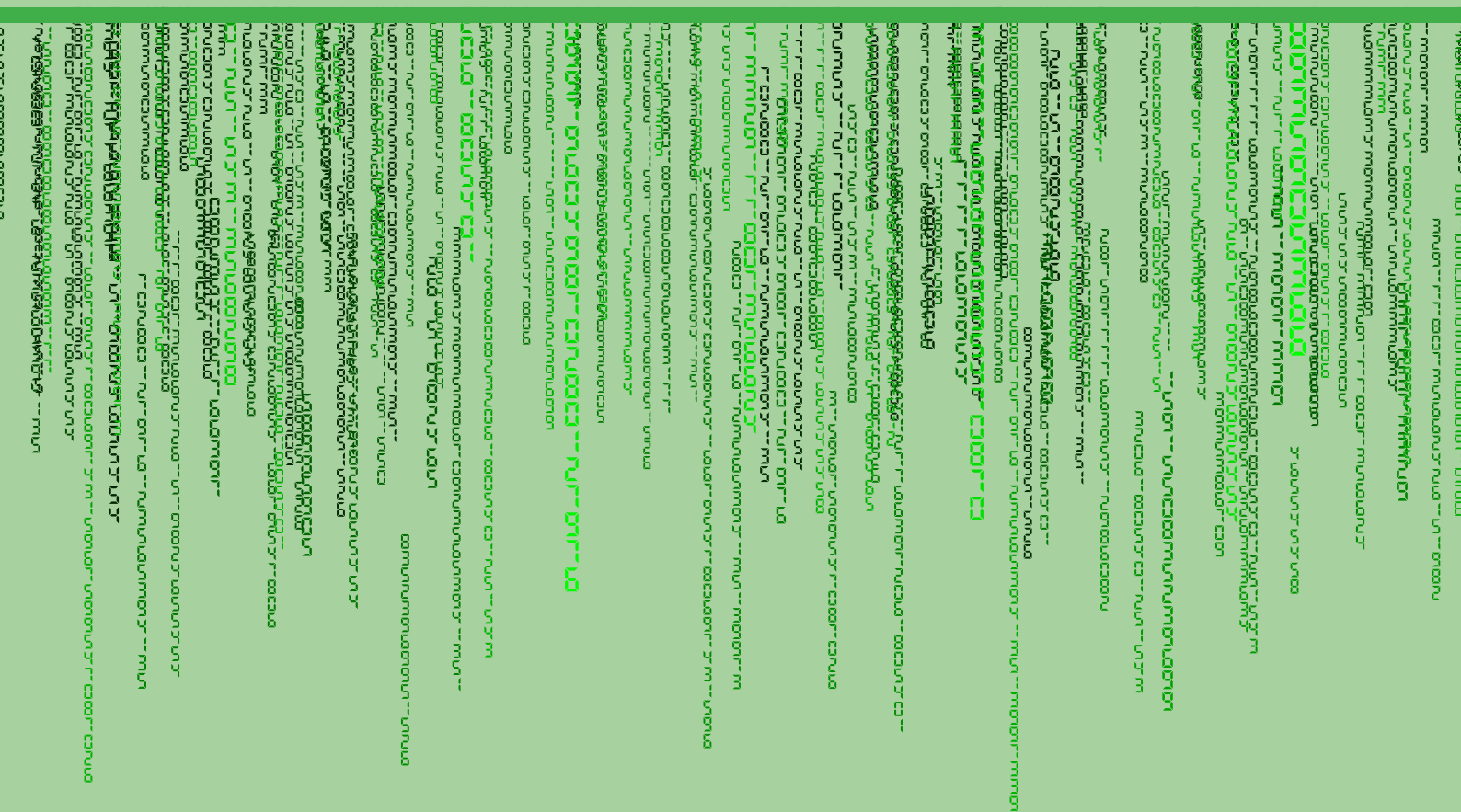
CONFINDUSTRIA EMILIA
AREA CENTRO: le imprese di Bologna, Ferrara e Modena

IL TRATTAMENTO DEI DATI PERSONALI

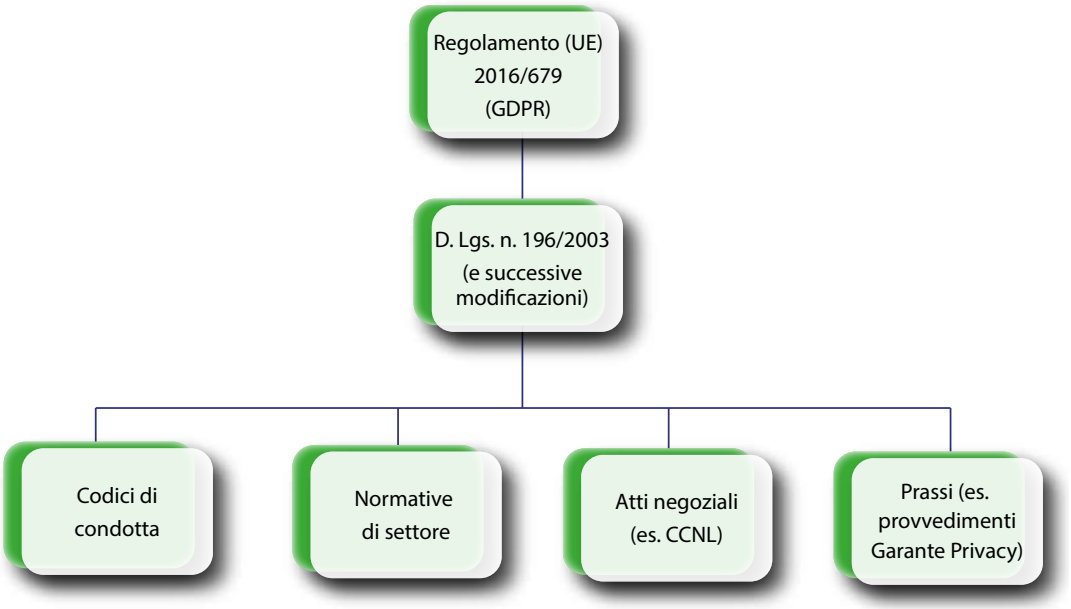
aggiornato a Febbraio 2019



A cura
Area Relazioni Industriali e Lavoro

INDICE

IL QUADRO DELLE FONTI

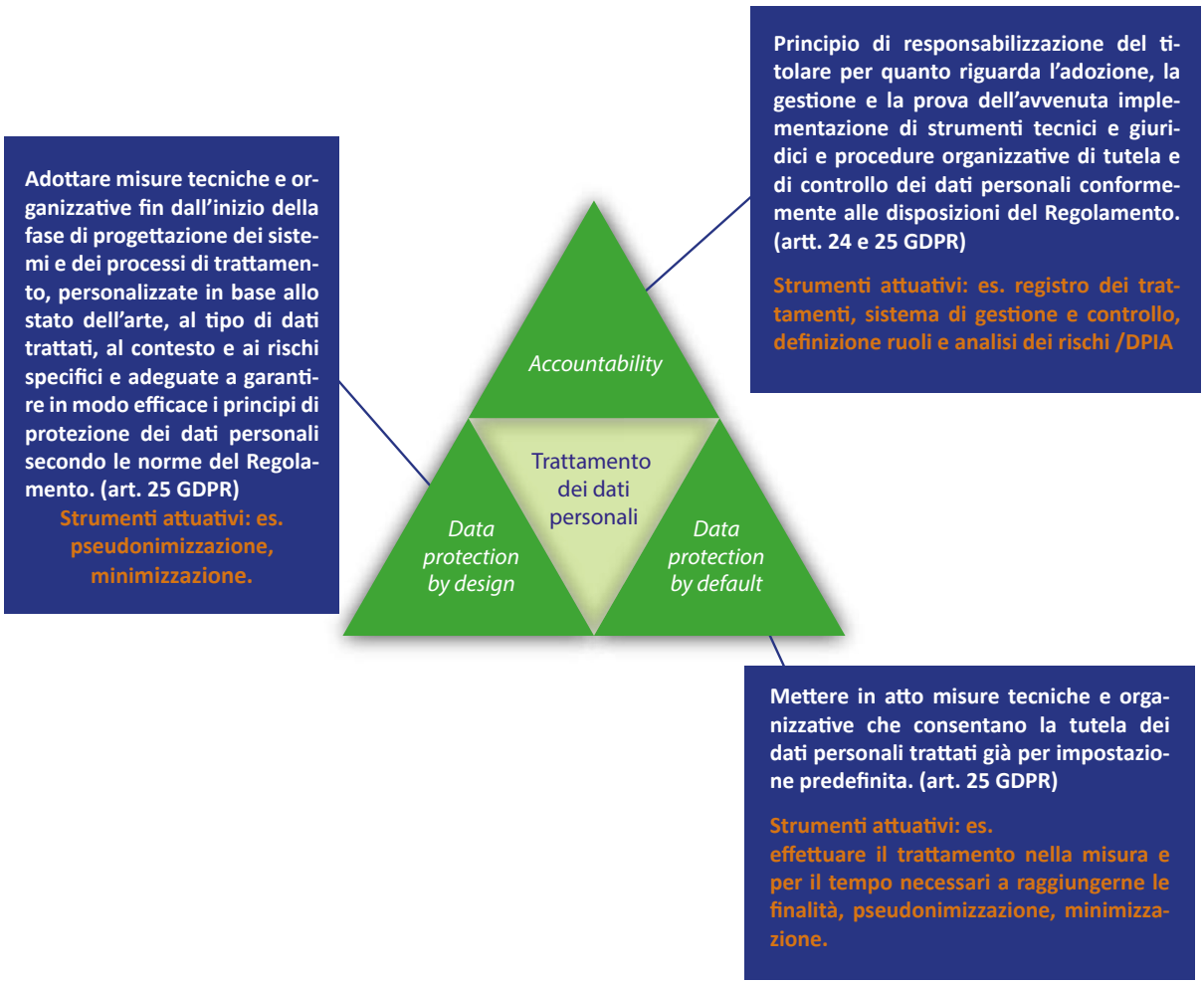


AMBITO DI APPLICAZIONE DEL REGOLAMENTO (UE) 2016/679 (GDPR)

Materiale *(art. 2, GDPR)*	**Trattamenti automatizzati** (anche parzialmente) **e non** automatizzati di **dati personali** purché conservati o destinati alla conservazione in un archivio, ad eccezione di quelli di cui all'art. 2 co. 2 del GDPR.
Territoriale *(art. 3, GDPR)*	Trattamenti di dati personali: • **realizzati nell'ambito delle attività di un soggetto stabilito nell'UE, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'UE;** • di **persone che si trovano nell'UE effettuati da soggetti non stabiliti nell'UE** per scopi di a) **offerta** di **beni** o **prestazione di servizi nell'UE**, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; b) **monitoraggio** del comportamento di **persone fisiche** che ha luogo nell'UE; • effettuati in territori **non UE ma soggetti al diritto dell'UE**.

NUOVI PRINCIPI CHIAVE: UN APPROCCIO INNOVATIVO

La sicurezza dei dati personali si realizza attraverso l'adozione di adeguate «misure tecniche o organizzative» da parte del titolare e del responsabile del trattamento. La nuova policy prevista dal Regolamento è di implementare misure non più "minime", bensì "idonee, adeguate ed opportune", al fine di commisurare la struttura tecnico-organizzativa alla tipologia di trattamento, alla natura del dato ed al livello di rischio (accountability).
L'adozione di un adeguato sistema organizzativo e di sicurezza contribuisce alla dimostrazione della conformità normativa, rispondendo al principio di "integrità, riservatezza dei dati, disponibilità e resilienza dei servizi di trattamento" (art. 32. l. b, GDPR).



DATO PERSONALE

Definizione *(art. 4, GDPR)*	"Qualsiasi **informazione** riguardante una **persona fisica identificata** o **identificabile** («interessato»)". È identificabile chi può essere individuato direttamente o indirettamente, soprattutto con dati come il nome o un numero identificativo, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Categorie particolari di dati personali *(art. 9, GDPR; artt. 2- sexies, 2- septies e 2- octies, D.Lgs. n. 196/2003)*	Dati relativi a **origine razziale** o **etnica**, **opinioni politiche**, **convinzioni religiose o filosofiche**, **appartenenza sindacale**, **salute**, **vita sessuale**, **orientamento sessuale**, **dati genetici**, **dati biometrici intesi a identificare in modo univoco una persona fisica**. Il GDPR prevede una disciplina specifica per le condizioni del trattamento sia di tale tipologia di dati (art. 9, co. 2 del GDPR) che di quelli relativi a condanne penali e reati o a connesse misure di sicurezza (art. 10 del GDPR). La normativa italiana prevede disposizioni per il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante, nonché per il trattamento di dati personali relativi a condanne penali e reati o alle relative misure di sicurezza.

TRATTAMENTO DEI DATI PERSONALI

Definizione *(art. 4, GDPR)*	"**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" (es. raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione).
Base giuridica *(art. 6, GDPR)*	Il trattamento è **lecito** solo se ricorre **almeno una** delle seguenti condizioni: • "consenso al trattamento espresso dall'interessato per una o più specifiche finalità" (lett. a); • "è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso" (lett. b); • "è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (lett. c); • "è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica" (lett. d); • "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (lett. e); • "è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi", sempre che gli interessi o i diritti e le libertà fondamentali dell'interessato non risultino prevalenti (specie nel caso di minori) (lett. f).
Principi del trattamento *(art. 5, GDPR)*	Il trattamento dei dati deve rispettare i seguenti principi: • **liceità**, **correttezza e trasparenza**: i dati devono essere trattati "in modo lecito, corretto e trasparente nei confronti dell'interessato" (lett. a); • **limitazione della finalità**: "raccolta per finalità determinate, esplicite e legittime", e trattati compatibilmente con le finalità (lett. b); • **minimizzazione dei dati**: adeguatezza, pertinenza e limitazione della tipologia dei dati rispetto alle finalità del trattamento (lett. c); • **esattezza**: esattezza e aggiornamento dei dati, con adozione delle misure necessarie (nei limiti della ragionevolezza) per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità del trattamento (lett. d); • **limitazione della conservazione**: conservazione dei dati in modo da consentire l'identificazione degli interessati per un periodo non eccedente rispetto al conseguimento delle finalità del trattamento, la conservazione per periodi più lunghi è ammessa solo per alcune finalità e con le modalità previste dalla seconda parte della medesima disposizione (lett. e); • **integrità e riservatezza**: garanzia, anche con misure tecniche e organizzative idonee, di sicurezza e protezione dei dati in modo che non siano soggetti a trattamenti non autorizzati o illeciti e che non si perdano, distruggano o danneggino accidentalmente (lett. f).

MISURE DI SICUREZZA

Prescrizioni *(art. 32, GDPR)*	Il titolare e il responsabile del trattamento devono mettere "**in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**" e nel "**valutare l'adeguato livello di sicurezza**" devono tener conto "in special modo dei rischi di distruzione, perdita, modifica, divulgazione non autorizzata o accesso accidentale o illegale ai dati personali trasmessi, conservati o comunque trattati". Esse devono comprendere, tra le altre, se del caso: a) "la pseudonimizzazione e la cifratura dei dati personali"; b) "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"; c) "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico"; d) "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento". Nel caso in cui il trattamento di dati personali presenti rischi specifici per i diritti e le libertà degli interessati (come ad esempio per il trattamento dei dati di minori), le misure tecniche e organizzative ulteriori sono individuate tramite la valutazione d'impatto preliminare (Data Protection Impact Assessment - DPIA).
Tipologie ed esempi	Possono essere suddivise in **tre** differenti **categorie**: **Misure tecniche** Ad esempio le misure di protezione delle architetture di rete, degli applicativi e delle banche dati e di protezione durante la trasmissione dei dati, tra le quali: • autenticazione informatica; • password e relative policy di gestione; • gestione delle utenze; • sistema di autorizzazione e configurazione dei profili; • antivirus e antispam; • back up; • pseudonimizzazione/anonimizzazione. **Misure fisiche** Ad esempio le misure di protezione delle aree, dei locali e degli archivi, per la protezione dall'accesso intenzionale e non autorizzato ai locali e agli archivi, tra le quali: • armadi chiusi a chiave o blindati; • distruzione fisica archivi cartacei; • controllo accessi (badge, reception e registrazione visitatori); • vigilanza. **Misure organizzative** Ad esempio le misure per l'assegnazione di compiti e responsabilità (nomine); per la costituzione e il consolidamento di una cultura aziendale relativa alle tematiche di tutela dei dati, per garantire che i trattamenti di dati personali avvengano per finalità autorizzate e consentite, tra le quali: • informativa e consenso; • Data Retention/cancellazione dei dati; • Incident Management; • gestione Data Breach; • Risk Assessment/Data Protection Impact Analysis (DPIA); • Change Management; • formazione di dipendenti e collaboratori in ambito Data Protection; • attribuzione incarichi e autorizzazioni.

Pseudonimizzazione *(art. 4, GDPR)*	Modalità di trattamento con la quale **i dati personali vengono resi anonimi e non attribuibili ad un interessato** a meno che non si integrino i dati con altre informazioni aggiuntive, che devono a loro volta essere conservate separatamente e sottoposte a misure tecniche e organizzative che garantiscano la loro non riconducibilità ad una persona fisica identificata o identificabile. È idonea a **minimizzare i rischi per gli interessati** e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati, ma la sua previsione non è preclusiva dell'adozione di misure di protezione differenti.

ALCUNE TIPOLOGIE SPECIFICHE DI TRATTAMENTO

Profilazione *(artt. 4 e 22, GDPR)*	Qualsiasi forma di **trattamento automatizzato** di dati personali che si sostanzia nell'utilizzo di tali dati per valutare determinati aspetti di una persona fisica (es. rendimento professionale, situazione economica, salute, preferenze personali, interessi, affidabilità, comportamento, spostamenti o ubicazione). Implica l'osservanza di oneri e l'attuazione di **tutele rafforzati** con riferimento sia alle misure tecnico-organizzative adottate, sia ai diritti degli interessati (vd. anche processi decisionali automatizzati, art. 22 del GDPR).
Discipline specifiche *(artt. 50 - 140, D. Lgs. n. 196/2003)*	La **legislazione nazionale disciplina** in maniera **specifica** i trattamenti di dati personali nei seguenti ambiti: giudiziario, difesa e sicurezza dello Stato, pubblico, sanitario, istruzione, archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici, rapporto di lavoro, comunicazioni elettroniche, giornalismo e libertà di informazione e espressione, marketing.
Trattamento dei dati personali nel rapporto di lavoro *(art. 88, GDPR; artt. 111, 111-bis, 113, 114 e 115, D. Lgs. n. 196/2003)*	Gli **Stati possono adottare**, con **legge** o **contratti collettivi**, **norme più specifiche** per finalità di: assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione, parità e diversità, salute e sicurezza, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, cessazione del rapporto di lavoro. Tali norme devono altresì prevedere misure specifiche di tutela, in particolare in tema di trasparenza del trattamento, trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e sistemi di monitoraggio sul posto di lavoro. La normativa italiana non apporta sostanziali modifiche rispetto alla disciplina previgente. In particolare, delega al Garante per la protezione dei dati personali la promozione dell'adozione di regole deontologiche per soggetti pubblici e privati che effettuino trattamenti di dati personali in tale ambito e richiama le disposizioni di cui agli artt. 4 e 8 della L. 300/1970 (Statuto dei lavoratori) e l'art. 10 del D. Lgs. n. 276/2003.

CONSENSO

Requisiti generali *(artt. 4, 7 e 8, GDPR; art. 2-quinquies, D.Lgs. n. 196/2003)*	Deve essere: **libero**, **specifico**, **informato**, **inequivocabil**e, **manifestato con dichiarazione o azione positiva**, **dimostrabile dal titolare**. Per i **dati ex art. 9 del GDPR e per i processi decisionali basati su trattamenti automatizzati (compresa la profilazione)** deve essere **esplicito**. Nel caso in cui i dati siano raccolti per **più finalità**, è necessario il **consenso per ognuna** di esse. Nel valutare se il consenso è stato prestato liberamente, si tiene conto del fatto che l'esecuzione di un contratto sia condizionata alla prestazione del consenso al trattamento di dati personali. Il consenso dei minori, per quanto riguarda l'offerta diretta nei loro confronti di servizi della società dell'informazione, in Italia, è valido a partire dai 14 anni (prima è necessario quello di chi esercita la potestà genitoriale).
Forma *(art. 7 par. 2, GDPR)*	La forma scritta non è imposta, **ma è idonea a garantire e provare** il rispetto delle condizioni necessarie. La richiesta del consenso al trattamento dovrà essere chiaramente **distinta** da altre materie, **semplice**, **chiara**, **facilmente accessibile e comprensibile**.
Revoca *(art. 7 par. 3, GDPR)*	Il consenso può essere **sempre revocato**, **con facilità analoga a quella con cui è stato prestato (no modalità più gravose)** e il **diritto** di revoca deve essere reso **conoscibile** all'interessato.

INFORMATIVA

Forma *(art. 12, GDPR)*	Deve essere **concisa**, **trasparente**, **intellegibile**, facilmente **accessibile** da parte dell'interessato e resa in un **linguaggio chiaro e semplice**. Resa di **norma per iscritto** "o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi la sua identità". Devono comunque essere rispettate tutte le sue caratteristiche. I casi di esonero dall'informativa sono tassativamente indicati dal GDPR.
Tempi *(artt. 13 e 14, GDPR)*	Deve essere rilasciata: • **al momento in cui i dati sono ottenuti**; • per i dati non raccolti direttamente presso l'interessato, entro un termine ragionevole comunque **non superiore a 1 mese dalla raccolta** oppure, nel caso i dati siano destinati alla comunicazione con l'interessato, massimo al momento della prima comunicazione all'interessato; oppure se è prevista la comunicazione ad altro destinatario, al massimo al momento della prima comunicazione dei dati.
Contenuto *(artt. 13 e 14, GDPR)*	Indicato tassativamente dal Regolamento, varia a seconda che i dati personali siano raccolti presso l'interessato o meno. Il **titolare** del trattamento deve in ogni caso indicare: • **l'identità** e i **dati** di **contatto propri** e dell'eventuale **rappresentante** nonché i **dati** di **contatto** del **DPO**;

segue ***Contenuto***	• le **finalità e la base giuridica del trattamento**; • **l'interesse** legittimo se costituisce base giuridica del trattamento; • **i destinatari dei dati o le categorie degli stessi e l'eventuale intenzione di operare un trasferimento** di dati in Paesi terzi e gli strumenti adottati se effettuato; • il periodo di **conservazione** oppure, se non è possibile, eventuali criteri di definizione di tale periodo; • i **trattamenti automatizzati** se effettuati, le relative logiche di funzionamento e le ripercussioni sull'interessato; • **i diritti degli interessati**, inclusi quelli relativi al reclamo a un'autorità di controllo e alla revoca del consenso (se il trattamento si fonda su tale base); • "se la comunicazione di dati personali è **un obbligo legale o contrattuale** oppure un requisito **necessario** per la **conclusione di un contratto**, e se l'interessato ha **l'obbligo di fornire i dati** personali nonché le **possibili conseguenze** della **mancata comunicazione** di tali dati" (se i dati sono raccolti direttamente presso l'interessato); • le **categorie** di **dati** personali, la loro **fonte** e, **l'eventualità** che i dati provengano da fonti **accessibili** al pubblico (se i dati non sono raccolti direttamente presso l'interessato). Nel caso in cui i dati debbano essere trattati per una **diversa finalità**, è necessario **informare l'interessato** prima di procedere al trattamento.

DIRITTI DEGLI INTERESSATI

Quali sono *(artt. 15, 16, 17, 18 e 20, GDPR)*	• Diritto di **accesso**; • Diritto di **rettifica**; • Diritto alla **cancellazione** (diritto all'oblio); • Diritto alla **limitazione** del trattamento; • Diritto alla **portabilità** dei dati.
Modalità di esercizio *(artt. 11 e 12, GDPR; art. 2-undecies, D. Lgs. n. 196/2003)*	Il titolare del trattamento, con la collaborazione del responsabile del trattamento, deve favorire l'esercizio dei diritti degli interessati. All'interessato che avanza una richiesta nell'esercizio di un suo diritto, il titolare deve dare **riscontro** al massimo **entro un mese dalla richiesta**, anche in caso di non ottemperanza motivata. La risposta fornita all'interessato deve essere **concisa**, **trasparente**, **intellegibile**, facilmente **accessibile** da parte dell'interessato e resa in un linguaggio chiaro e semplice. **L'esercizio** di tali diritti è **limitato**, secondo la normativa nazionale, se ne deriva un **pregiudizio** effettivo e concreto a: a) interessi tutelati dalla normativa **antiriciclaggio**; b) interessi tutelati dalla normativa a sostegno alle **vittime di estorsione**; c) attività di **Commissioni parlamentari** d'inchiesta; d) attività svolte da un **soggetto pubblico** per esclusive finalità inerenti alla **politica monetaria e valutaria**, al sistema dei **pagamenti**, al controllo degli **intermediari** e dei **mercati** creditizi e finanziari, e alla tutela della loro stabilità; e) allo svolgimento delle **investigazioni difensive** o all'esercizio di un **diritto in sede giudiziaria**; f) alla **riservatezza** dell'identità del **dipendente** che **segnala l'illecito** di cui sia venuto a conoscenza in ragione del proprio ufficio.

SOGGETTI

Titolare del trattamento *(artt. 4, 24, 25, 26 e 27, GDPR)*	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che singolarmente o con altri **determina finalità e mezzi del trattamento** e nei confronti del quale l'interessato può esercitare i suoi diritti. Conformemente ai principi di ***accountability, data protection by design e by default*** e tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e dei rischi connessi, **attua misure** tecniche e organizzative **idonee a garantire e a dimostrare, il rispetto delle regole e dei principi del GDPR**, sia con riferimento al momento di determinare i mezzi del trattamento, sia al momento stesso del trattamento. **Riesamina** e **aggiorna le misure** se necessario. Può **aderire** ai **codici di condotta** (art. 40 del GDPR) o al **meccanismo di certificazione** (art. 42 del GDPR) per dimostrare il rispetto degli obblighi imposti dal GDPR. Se due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento, il GDPR prevede che essi siano **contitolari del trattamento,** che determinano tramite accordo interno i rispettivi ruoli, responsabilità e funzioni. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato che può esercitare i propri diritti nei confronti di ciascun contitolare indipendentemente dalle disposizioni dell'accordo.
Responsabile del trattamento *(artt. 4, 27 par. 1, 28, 29, 30 par. 2, 33 par. 2 e 37 par. 1, GDPR)*	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che **tratta i dati personali per conto del titolare**. È **designato dal titolare** con un **contratto** (o altro atto giuridico) in cui sono disciplinati i suoi rapporti con il titolare stesso e definiti i suoi compiti così come individuati dal GDPR (art. 28, par. 3). Deve presentare garanzie sufficienti per attuare misure tecniche e organizzative conformi al GDPR (vale a dire essere dotato di **sufficienti capacità e competenze** atte alla realizzazione dello scopo per cui la figura è istituita) ed essere **istruito** dal titolare. La sua **attività** è **prevalentemente strumentale rispetto a quella del titolare,** ma se determina le finalità e i mezzi del trattamento è considerato titolare del trattamento in questione, anche per quanto riguarda i relativi profili di responsabilità in caso di violazioni del GDPR. Può avvalersi di **sub-responsabili** previa autorizzazione scritta, specifica o generale, del titolare. I sub-responsabili dovranno essere investiti del ruolo mediante un contratto avente caratteristiche analoghe a quello che regola i rapporti tra titolare e responsabile. In caso di inadempimento del sub-responsabile, il responsabile conserva la responsabilità dell'adempimento nei confronti del titolare.
Rappresentante nell'Unione del titolare o del responsabile *(art. 27, GDPR)*	**Designato** per iscritto dal **titolare** del trattamento o dal **responsabile** del trattamento, nei **casi di cui all'articolo 3**, **par. 2 del GDPR** (e ad eccezione dei casi di cui all'art. 27, par. 2). È stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato. La sua funzione primaria è quella di **interloquire con le autorità di controllo** e con gli interessati, per tutte le questioni riguardanti il trattamento, **sostituendosi o affiancando il titolare o il responsabile**. Sono fatte salve le azioni legali che potrebbero essere promosse nei confronti del titolare o del responsabile.

Soggetti istruiti o autorizzati *(art. 29, GDPR; art. 2 - quaterdecies, D. Lgs. n.196/2003)*	**Persone fisiche autorizzate** che, **istruite** dal titolare e sotto la diretta autorità sua o del responsabile del trattamento, **abbiano accesso ai dati** personali. In particolare, il titolare o il responsabile del trattamento, individuate le modalità di autorizzazione più opportune, possono designare espressamente, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, persone fisiche per svolgere specifici compiti e funzioni relativi al trattamento di dati personali.
Data Protection Officer - Responsabile per la protezione dei dati *(artt. 4, 37, 38 e 39, GDPR)*	**Persona fisica o giuridica, interna** (dipendente del titolare) **o esterna** (mediante contratto di servizi) all'azienda/ente/ecc., designato in funzione di adeguate **competenze** professionali (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e capacità di svolgere i compiti ad esso attribuiti dal GDPR) e **privo di conflitti di interessi**. Opera **senza ricevere istruzioni** sull'esecuzione dei suoi compiti. Deve essere **tempestivamente e adeguatamente coinvolto** in tutte le questioni riguardanti la protezione dei dati personali e **dotato** dal titolare e dal responsabile delle **risorse necessarie** per **assolvere** i propri **compiti**, **accedere** ai dati personali e ai trattamenti e **mantenere** la propria conoscenza **specialistica**. **Non può essere penalizzato o rimosso dal titolare** o dal responsabile per aver adempiuto alle proprie funzioni. Riferisce direttamente al vertice gerarchico del titolare o del responsabile. La sua nomina è necessaria quando: • il trattamento è effettuato da **un'autorità o un organismo pubblico** (tranne autorità giurisdizionali); • le attività principali del titolare del trattamento o del responsabile del trattamento consistono in **trattamenti** di **dati personali** che per la loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico** degli interessati su **larga scala**; • le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento su larga scala di dati "sensibili"** di cui all'art. 9 del GDPR o dati giudiziari relativi a condanne penali o reati di cui all'art. 10 del GDPR. Ha il **compito di**: • **informare** e **fornire consulenza** al titolare o al responsabile del trattamento nonché ai soggetti autorizzati in relazione agli obblighi del GDPR o di altre disposizioni dell'Unione o degli Stati membri attinenti alla tutela dei dati; • **sorvegliare** l'osservanza del GDPR o di altre disposizioni a tutela dei dati; • fornire **parere** se richiesto in merito alla **valutazione di impatto** e **sorvegliarne** lo svolgimento; • **cooperare** con le **autorità di controllo** e fare da tramite tra queste e l'azienda/ente, ecc. I **suoi dati** di contatto sono **pubblicati e comunicati** all'autorità di controllo dal titolare o dal responsabile del trattamento. Gli **interessati possono contattarlo** per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.
Amministratore di Sistema *(Provvedimenti Garante privacy del 27/11/2008 e del 25/6/2009)*	**Non esistono definizioni** normative e tecniche **condivise**. Secondo il Garante per la protezione dei dati personali, l'amministratore di sistema è una figura professionale che **si occupa della gestione e della manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali**, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning), le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Non rientrano invece nella definizione coloro che intervengono sui sistemi di elaborazione e sui sistemi software solo occasionalmente (es. manutenzione).

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

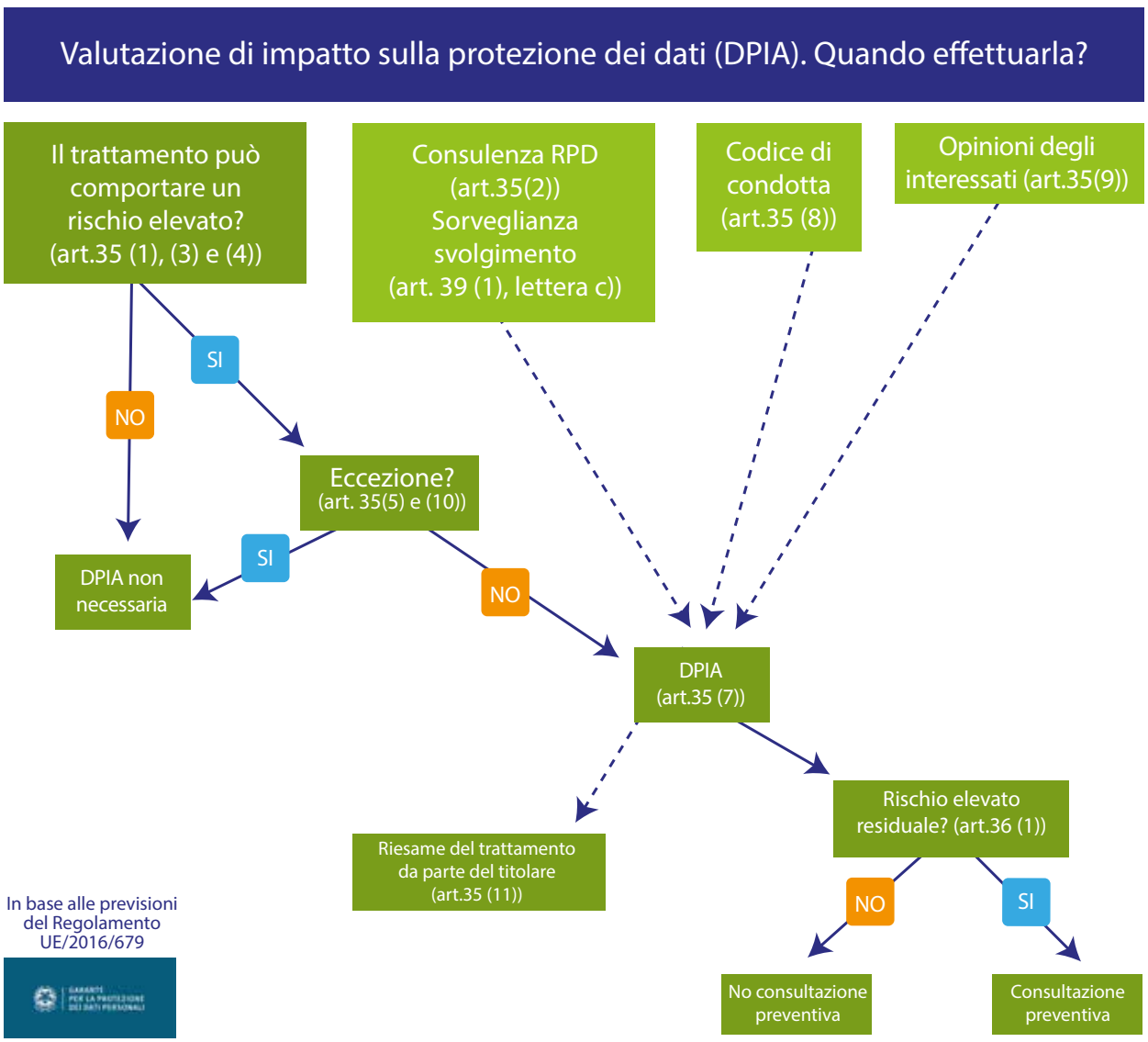
Cos'è	Strumento che consente di **tracciare costantemente i trattamenti** dei dati personali effettuati a fini non solo difensivi, ma anche di monitoraggio, aggiornamento e valutazione del rischio dei processi aziendali che implicano il trattamento di tali dati, coerentemente con in principi di **accountability**, **data protection by design e data protection by default**.
Forma e contenuti *(art. 30, GDPR; Istruzioni del Garante privacy v. comunicato stampa 8/10/2018 e FAQ)*	Deve essere tenuto in **forma scritta**, anche in formato elettronico e contenere: • nel caso del **registro del titolare** del trattamento (e suo rappresentante): a) il nome e i dati di contatto del **titolare** del trattamento, del contitolare, dell'eventuale rappresentante del titolare del trattamento e del DPO; b) le **finalità** del trattamento; c) una **descrizione** delle **categorie** di **interessati** e delle categorie di **dati personali**; d) le **categorie** di **destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; e) i **trasferimenti** di dati personali verso un Paese terzo o un'organizzazione internazionale; f) i termini previsti per la **cancellazione** delle diverse categorie di dati; g) una **descrizione** generale delle **misure di sicurezza** tecniche e organizzative; • nel caso di **registro** del **responsabile** del trattamento (e del suo rappresentante): a) il **nome** e i **dati** di **contatto** del responsabile/i, di ogni titolare del trattamento per conto del quale si trattano i dati e del suo eventuale rappresentante o del responsabile del trattamento nonché del **DPO**; b) le **categorie** dei **trattamenti** effettuati per conto di ogni titolare del trattamento; c) eventuali **trasferimenti** di **dati** personali verso un **Paese terzo** o un'organizzazione internazionale; d) quando possibile, una **descrizione** generale delle **misure** di **sicurezza** tecniche e organizzative di cui all'articolo 32 del GDPR. Il Garante per la protezione dei dati personali indica, tra l'altro, quali informazioni deve contenere il registro, le modalità di conservazione e aggiornamento e fornisce modelli di registro semplificato per titolari e responsabili nelle PMI.
Soggetti obbligati *(art. 30, GDPR; Istruzioni del Garante privacy v. comunicato stampa 8/10/2018 e FAQ)*	Tutti i titolari del trattamento e i responsabili del trattamento con più di 250 dipendenti o, indipendentemente dal numero dei dipendenti, che effettuano trattamenti rischiosi per i diritti e le libertà dell'interessato, **non occasionali** o relativi a dati sensibili o giudiziari. Il **Garante** per la protezione dei dati personali **ha specificato che**: • sono tenuti a redigere il registro i titolari e i responsabili del trattamento **fino a 250 dipendenti che effettuino trattamenti che possano presentare rischi, anche non elevati**, per i diritti e le libertà delle persone o che effettuino trattamenti non occasionali di dati oppure trattamenti di particolari categorie di dati (come i dati biometrici, dati genetici, quelli sulla salute, sulle convinzioni religiose, sull'origine etnica etc.), o anche di dati relativi a condanne penali e a reati;

segue ***Soggetti obbligati***	• le imprese e organizzazioni con **meno di 250 dipendenti obbligate** alla tenuta del registro potranno comunque beneficiare di alcune **misure di semplificazione**, potendo circoscrivere l'obbligo di redazione del registro alle sole specifiche attività di trattamento di cui sopra (es. ove il trattamento delle categorie particolari di dati si riferisca a quelli inerenti ad un solo lavoratore dipendente, il registro potrà essere predisposto e mantenuto esclusivamente con riferimento a tale limitata tipologia di trattamento); • la **redazione** del registro è **raccomandata a tutti** i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce ad attuare meglio, con modalità semplici e accessibili a tutti, il principio di accountability e ad agevolare in maniera dialogante e collaborativa l'attività di controllo del Garante stesso. Il Garante invita altresì a consultare il documento interpretativo del 19 aprile 2018 del Gruppo art. 29 (ora Comitato europeo per la protezione dei dati).

VALUTAZIONE DI IMPATTO (DPIA)

Cos'è *(artt. 35 par. 1 e 35 par. 2, GDPR)*	Specifica **procedura di valutazione del rischio** che il **titolare** del trattamento, anche **consultando** il **DPO** se presente, deve effettuare **preventivamente**, quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto di natura, oggetto, contesto e finalità del trattamento stesso. Nell'ambito di una stessa valutazione possono essere esaminati un insieme di trattamenti simili che presentano rischi elevati analoghi.
Quando farla *(art. 35 par. 3, GDPR; Linee Guida Gruppo art. 29 (WP248, rev. 01); Garante privacy, provvedimento n. 467, 11/10/2018, all.1)*	La valutazione di impatto è richiesta **in particolare** quando si intendono effettuare: a) una **valutazione sistematica e globale** di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il **trattamento**, su **larga scala**, di **categorie particolari** di dati personali di cui all'articolo 9, par. 1 del GDPR, o di dati relativi a condanne penali e a reati di cui all'articolo 10 del GDPR; c) la **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico. Secondo le indicazioni del Gruppo art. 29, "al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto […] in virtù del loro rischio elevato intrinseco, […] si devono considerare i seguenti nove criteri: 1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione 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 dell'interessato"; 2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3. monitoraggio sistematico degli interessati;

segue ***Quando farla***	4. dati sensibili o giudiziari o dati aventi carattere altamente personale; 5. trattamento di dati su larga scala; 6. creazione di corrispondenze o combinazione di insiemi di dati; 7. dati relativi a interessati vulnerabili; 8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; 9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto". Il Gruppo art. 29 specifica inoltre che "nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che **soddisfi due criteri debba formare oggetto di una valutazione d'impatto** sulla protezione dei dati. In generale, il WP29 ritiene che **maggiore è il numero di criteri** soddisfatti dal trattamento, **più è probabile che sia presente un rischio elevato** per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare. Tuttavia, in alcuni casi, **un titolare può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto** sulla protezione dei dati". Inoltre, il Garante per la protezione dei dati personali ha predisposto un elenco delle tipologie di trattamento da sottoporre a valutazione d'impatto sulla base del WP248, rev. 01, allo scopo di specificarne ulteriormente il contenuto e a complemento dello stesso. L'elenco "è riferito esclusivamente a tipologie di trattamento soggette al meccanismo di coerenza" previsto dal GDPR e non è esaustivo.
Procedura (*art. 35 par. 7 e 36, GDPR)*	La formalizzazione della valutazione deve **contenere** almeno: • **descrizione** sistematica dei **trattamenti** previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento; • valutazione della **necessità** e **proporzionalità** dei trattamenti in relazione alle finalità; • **valutazione dei rischi** per i diritti e le libertà degli interessati; • descrizione delle **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. Se, all'esito della valutazione, emergesse **un rischio elevato del trattamento in assenza di misure adottate dal titolare per attenuare tale rischio**, quest'ultimo consulta il Garante per la protezione dei dati personali, comunicando contestualmente tra l'altro, oltre alla Valutazione di impatto, finalità e mezzi del trattamento e misure previste per la minimizzazione del rischio. Nel caso in cui l'Autorità riscontri delle inadempienze rispetto agli standard imposti dal GDPR, fornisce entro un termine di 8 settimane, prorogabile a seconda della complessità, un parere scritto al quale il titolare è tenuto a conformarsi.



DATA BREACH NOTIFICATION

Cos'è *(art. 33 par.1, GDPR)*	Procedura di **segnalazione di violazioni** alla quale è tenuto qualunque **titolare** del trattamento che riscontri una violazione dei sistemi e delle procedure attuate a tutela dei dati personali.
Procedura *(artt. 33 e 34, GDPR)*	Il titolare del trattamento deve **notificare**: • **all'Autorità** di controllo, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, le violazioni di dati personali, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, dovrà essere corredata dei **motivi del ritardo**; • **all'interessato**, senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone. Il responsabile del trattamento che viene a conoscenza di un'eventuale violazione, è tenuto a informare tempestivamente il titolare in modo che possa procedere agli adempimenti di sua competenza.

Notifica *(artt. 33 e 34, GDPR)*	Deve: • indicare la **natura** della violazione dei dati personali, le **categorie** e il **numero** approssimativo di **interessati** in questione (solo per notifica all'Autorità), i dati di **contatto** del **DPO** o di altro punto di contatto presso cui ottenere più informazioni; • descrivere **le probabili conseguenze della violazione** nonché le **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi.

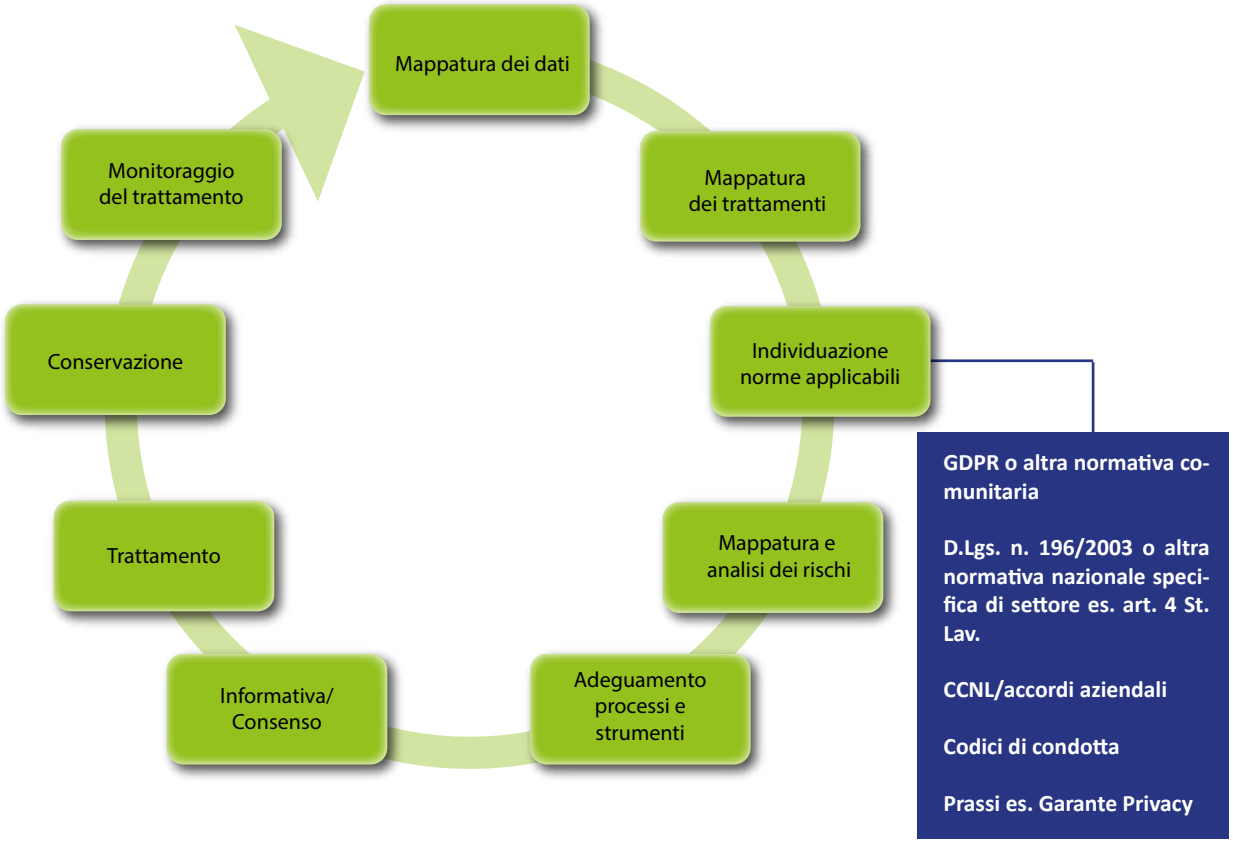
TRASFERIMENTO DEI DATI ALL'ESTERO

Principio generale *(art. 44 GDPR)*	"**Qualunque trasferimento** di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un Paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un Paese terzo o un'organizzazione internazionale verso un altro Paese terzo o un'altra organizzazione internazionale, **ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni"** imposte dal GDPR.
Condizioni del trasferimento *(artt. 45, 46 e 47, GDPR)*	Il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale è ammesso: • mediante un atto di esecuzione con il quale la Commissione decide che il Paese terzo/l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche; • in mancanza della predetta decisione, solo se il titolare o il responsabile hanno fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Esemplificazioni di garanzie specifiche sono indicate all'art. 46, par. 2 e 3, tra le quali sono incluse le norme vincolanti d'impresa ex l'art. 47, un codice di condotta ex art. 40 del GDPR, un meccanismo di certificazione ex art. 42 del GDPR, (in questi ultimi due casi è necessario anche l'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel Paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati); • in via eccezionale, in mancanza delle condizioni precedenti soltanto nelle ipotesi di cui all'art. 49 del GDPR, tra le quali si ricordano, i casi in cui: a) **l'interessato** abbia esplicitamente acconsentito al trasferimento proposto, **previa informativa** dei possibili rischi dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; b) il trasferimento sia **necessario all'esecuzione di un contratto** concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato o per l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato.

SANZIONI

Quantificazione e criteri *(artt. 83 e 84, GDPR; artt. 167, 167-bis, 167-ter, 168 e 170, D.Lgs. n. 196/2003)*	Le autorità di controllo possono infliggere una **sanzione amministrativa** considerando, tra l'altro, la natura, la gravità e la durata della violazione; il carattere doloso o colposo della violazione, le misure adottate; il grado di responsabilità; eventuali precedenti violazioni; il grado di cooperazione; l'adesione ai codici di condotta o ai meccanismi di certificazione. Per ogni singola violazione non è definito un importo, ma solo un **massimale** della sanzione che può arrivare, a seconda delle diverse tipologie, **fino a 10 o 20 milioni di euro** o, per le **imprese**, **fino al 2% o 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore**. Il legislatore italiano ha inoltre introdotto nuove fattispecie di **illecito penale** che puniscono con la reclusione le **seguenti violazioni**: • illecito trattamento di dati personali in specifici settori (es. comunicazioni elettroniche); • illecito trattamento di particolari categorie di dati personali e violazioni delle relative misure di garanzia; • illecito trasferimento di dati personali all'estero; • illecita comunicazione e diffusione di dati personali trattati su larga scala; • acquisizione fraudolenta di dati personali trattati su larga scala; • false dichiarazioni al Garante o produzione di atti e documenti falsi; • interruzione dolosa o turbamento dell'esecuzione dei compiti ed esercizio dei poteri del Garante; • inosservanza di provvedimenti del Garante.

COSA FARE? UN ESEMPIO DI PROCESSO



ESEMPI DI DOMANDE PER UN'AUTO-DIAGNOSI

Dati oggetto del trattamento	1. In azienda sono trattati dati personali? Che tipo di dati sono trattati? 2. Sono trattate particolari tipologie di dati che richiedono tutele rafforzate? 3. I dati raccolti sono proporzionati alle finalità del trattamento? Quali sono realmente necessari?
Base giuridica	1. È stata individuata la base giuridica del trattamento? 2. Rientra tra quelle previste dal GDPR?
Trattamento dei dati personali	1. A quali fini vengono trattati i dati? 2. I trattamenti di dati personali sono effettivamente necessari? Qualcuno di essi potrebbe riguardare dati anonimi? 3. Vengono adottate misure per garantire la sicurezza del trattamento e l'integrità del dato trattato? Quali sono? 4. In azienda si effettuano trattamenti rischiosi dei dati come ad es. quelli automatizzati? 5. Si effettuano attività di videosorveglianza o geolocalizzazione? Sono conformi alle normative e alle indicazioni del Garante? 6. All'interessato è stata sottoposta l'informativa? 7. Gli interessati sono a conoscenza del trattamento effettuato, delle finalità e delle modalità dello stesso? 8. L'azienda mette l'interessato in condizione di esercitare i propri diritti previsti dal GDPR? 9. Viene verificata l'esattezza dei dati trattati? 10. I dati personali trattati vengono aggiornati periodicamente? Sono previsti meccanismi di cancellazione o rettifica tempestiva di dati inesatti rispetto alle finalità del trattamento? 11. Chi accede ai dati personali trattati e chi effettua i trattamenti? Sono stati previsti profili di autorizzazione? 12. Vengono effettuati trasferimenti di dati all'estero? Se si, vengono rispettati i presupposti di liceità e finalità?
Conservazione dei dati	1. Quali misure di sicurezza vengono adottate? 2. Per quanto tempo i dati personali vengono conservati? 3. Il periodo di conservazione è stato definito in conformità alle normative di riferimento oppure è eccessivo? 4. L'interessato è informato del periodo di conservazione? 5. Quando viene verificato il tempo di conservazione?
Informativa	1. L'informativa adottata contiene le informazioni necessarie, ad esempio quelle su: a. categorie e finalità dei dati trattati; b. base giuridica del trattamento dei dati/legittimi interessi perseguiti; c. possibilità o meno di rifiutare il conferimento dei dati; d. destinatari dei dati o loro categorie; e. trasferimento dei dati in Paesi terzi e, se effettuato, strumenti adottati; f. diritti dell'interessato; g. identificazione e dati di contatto del titolare del trattamento e del DPO; h. indicazione di trattamenti automatizzati, delle relative logiche e delle conseguenze per gli interessati. 2. Contiene le ulteriori informazioni specifiche da fornire a seconda che i dati siano stati raccolti direttamente presso l'interessato o meno?

Consenso degli interessati	1. Il format utilizzato esprime un consenso inequivocabile, libero, specifico, informato, verificabile, revocabile? 2. L'informativa prevede la possibilità di revocare il consenso qualora questo costituisca la base giuridica del trattamento? 3. Il consenso è richiesto per ogni autonoma finalità di trattamento?
I soggetti	1. Compiti e responsabilità dei diversi soggetti coinvolti sono definiti in maniera chiara? 2. Gli autorizzati sono stati correttamente individuati ed istruiti? 3. È necessario nominare il DPO? 4. Le competenze dei soggetti designati dal titolare sono adeguate ai vari ruoli conferiti? 5. Sono stati indicati e comunicati i dati di contatto di titolare e DPO agli interessati ed alle autorità di controllo quando previsto?
Il Registro dei trattamenti	1. È necessario tenerne uno? Se sì quello adottato contiene: a. dati del titolare del trattamento e, ove del caso, del contitolare e del responsabile della protezione dei dati; b. finalità del trattamento; c. descrizione delle categorie di interessati e delle categorie dei dati personali; d. categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali; e. trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale; f. termini previsti per la cancellazione delle diverse categorie di dati; g. descrizione generale delle misure di sicurezza tecniche e organizzative.
Valutazione d'impatto	1. L'uso delle tecnologie adottate presenta rischi in quanto vi sono: a. trattamenti automatizzati; b. dati sensibili; c. altro (v. specifica scheda su Valutazione di impatto - DPIA). 2. La valutazione adottata contiene: a. descrizione e valutazione dei trattamenti e finalità perseguite; b. valutazione dei rischi; c. misure previste ed adottate.

STAY TUNED

La materia è complessa e in divenire, sia dal punto di vista normativo/interpretativo che applicativo. È quindi fondamentale tenersi aggiornati. Puoi farlo qui:

Garante privacy ***https://www.garanteprivacy.it/***

EDPB – European Data Protection Board (Comitato europeo per la protezione dei dati, già Gruppo art. 29)
https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_it

Confindustria Emilia Area Centro tramite le nostre comunicazioni reperibili nell'area riservata agli associati accessibile dal sito ***www.confindustriaemilia.it*** oppure attraverso la nostra newsletter.

Finito di stampare
febbraio 2019