MANUALE PRIVACY GDPR

(Reg.UE 2016/679 – GDPR – General Data Protection Regulation)

VALIDAZIONE DEL DOCUMENTO		
Approvato da:	Titolare del trattamento	*IL PRESIDENTE - DOPOLAVORO ATAC COTRAL* ..... (Timbro/Firma)

SOMMARIO

1) PRINCIPI GENERALI IN MATERIA DI PROTEZIONE DEI DATI

1.1) Il diritto fondamentale alla protezione dei dati

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

Sulla base di tale principio l'Unione Europea ha ritenuto di emanare uno specifico Regolamento (**GDPR**), contenente i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali finalizzato a garantirne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il GDPR è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

1.2) I principi generali in materia di privacy

La scrivente organizzazione, in qualità di Titolare del trattamento, garantisce l'applicazione dei principi fondamentali della privacy, sanciti dal GDPR ed identificati nella seguente tabella.

PRINCIPIO GENERALEE RIF. LEGGE	DESCRIZIONE
LICEITÀ, CORRETTEZZA E TRASPARENZA (GDPR, Art.5, c.1, l.a)	Ogni trattamento di dati è legittimato da specifici requisiti, quali un consenso espresso dell'interessato, un obbligo di legge, un contratto tra le parti, un interesse legittimo del titolare. I dati sono trattati in modo corretto e trasparente nei confronti dell'interessato
FINALITÀ' (GDPR, Art.5, c.1, l.b)	I dati personali sono raccolti e trattati solo per finalità predeterminate, esplicite e legittime
NECESSITÀ', NON ECCEDENZA, ESSENZIALITÀ (GDPR, Art.5, c.1, l.c)	L'utilizzo dei dati personali è sempre ridotto al minimo necessario essenziale per il raggiungimento delle finalità dichiarate; i dati personali sono raccolti e trattati solo se funzionali al raggiungimento delle finalità dichiarate; i dati personali sono trattati con modalità e strumenti proporzionali alle finalità da raggiungere
ESATTEZZA, COMPLETEZZA, AGGIORNAMENTO (GDPR, Art.5, c.1, l.d)	I dati personali sono puntualmente verificati, in modo che sia garantita la loro esattezza, completezza ed aggiornamento
CONSERVAZIONE (GDPR, Art.5, c.1, l.e)	I dati personali sono conservati per un periodo di tempo limitato al raggiungimento delle finalità dichiarate
SICUREZZA (GDPR, Art.5, c.1, l.f)	i dati sono sempre raccolti e trattati previa adozione di idonee misure di sicurezza
RISERVATEZZA (GDPR, Art.5, c.1, l.f)	i dati sono trattati da soggetti adeguatamente identificati, autorizzati ed istruiti

Il presente manuale e relativi allegati, riportano adeguate e complete evidenze in merito ai suddetti principi generali, ottemperando al requisito di Accountability previsto dall'Art.5, comma 2 del GDPR ***("il Titolare è competente per il rispetto dei principi generali in materia di privacy ed in grado di comprovarlo")***

2) RIFERIMENTI NORMATIVI E DEFINIZIONI

2.1) Riferimenti normativi

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (**GDPR**, General Data Protection Regulation)
WEB:http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=IT

Il 4 maggio 2016, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi del **Regolamento europeo in materia di protezione dei dati personali** e della Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini. Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento, che diviene definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018. Il Regolamento porta significative innovazioni non solo per i cittadini, ma anche per aziende, enti pubblici, associazioni, liberi professionisti. Il Regolamento punta a rispondere alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dei Paesi dell'Unione europea. Tenuto conto della portata innovativa del Regolamento, nonché del suo ambito applicativo, esso viene ritenuto quale **framework di riferimento internazionale** per una corretta gestione delle attività di trattamento dei dati.

Di seguito una sintesi dei principi introdotti dal Regolamento

Imprese ed enti avranno più **responsabilità** (*accountability*), ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste sanzioni, anche elevate. Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale. Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione Europea.

Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue. Fra le principali novità del Regolamento c'è il cosiddetto «**sportello unico**» (*one stop shop*), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme. Salvo casi specifici, le imprese stabilite in più Stati o che offrono prodotti e servizi in vari Paesi dell'Ue, per risolvere possibili problematiche sull'applicazione e il rispetto del Regolamento potranno rivolgersi ad un solo interlocutore: cioè all'Autorità di protezione dei dati del Paese dove si trova il loro stabilimento principale.

Il Regolamento promuove la **responsabilizzazione** (*accountability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati. Il principio-chiave è «**privacy by design**» ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.
Ad esempio, è previsto l'obbligo di effettuare **valutazioni di impatto** (*Privacy Impact Assessment*) prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi. Viene inoltre introdotta la figura del «**Responsabile della protezione dei dati**» (*Data Protection Officer o DPO*), incaricato di assicurare una gestione corretta dei dati personali nelle imprese.

Il Regolamento introduce regole più chiare in materia di **informativa e consenso**, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (*data breach*).

L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti.
Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea.
Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; cosi come dovranno sapere che hanno il diritto di **revocare il consenso** a determinati trattamenti, come quelli a fini di marketing diretto.

Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli **standard di adeguatezza** in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.
Come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione europea, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti.
In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).

Il titolare del trattamento dovrà comunicare eventuali **violazioni dei dati personali** (*data breach*) all'Autorità nazionale di protezione dei dati.
Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative. L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

Grazie all'introduzione del cosiddetto «**diritto all'oblio**», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.

Normative comunitarie correlate:

- Articolo 8, paragrafo 1, della **Carta dei diritti fondamentali dell'Unione europea** («Carta») e Articolo 16, paragrafo 1, del **Trattato sul Funzionamento dell'Unione Europea** («TFUE»), che stabiliscono il principio generale secondo cui ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
- Parere del Comitato economico e sociale europeo sulla proposta della Commissione (GU C 229 del 31.7.2012, pag. 90).
- Parere del Comitato delle regioni sulla proposta della Commissione (GU C 391 del 18.12.2012, pag. 127).
- Posizione del Parlamento europeo del 12 marzo 2014; posizione del Consiglio in prima lettura dell'8 aprile 2016; posizione del Parlamento europeo del 14 aprile 2016.
- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).
- Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (C(2003) 1422) (GU L 124 del 20.5.2003, pag. 36).
- Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).
- Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Cfr. pagina 89 della presente Gazzetta ufficiale).
- Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico») (GU L 178 del 17.7.2000, pag. 1).
- Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori (GU L 95 del 21.4.1993, pag. 29).
- Regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativo alle statistiche comunitarie in materia di sanità pubblica e di salute e sicurezza sul luogo di lavoro (GU L 354 del 31.12.2008, pag. 70).
- Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).
- Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU L 351 del 20.12.2012, pag. 1).
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).
- Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).
- Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

Corrigendum del Consiglio UE	Il Consiglio dell'Unione Europea ha presentato il 19/04/2018 un documento estremamente corposo (385 pagine) di modifica del GDPR.

Interpretazioni e linee guida dell'Autorità Garante Italiana sul GDPR:

GDPR: Pagina Informativa Garante Italiano

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361

GDPR: Scheda Informativa sul DPO

http://www.garanteprivacy.it/rpd

GDPR: Prima Guida Informativa

http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati

GDPR: Guida Applicativa Garante Italiano

http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

Riferimenti alla normativa nazionale, in fase di armonizzazione:

- Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali.
- Allegato B: "Disciplinare tecnico in materia di misure minime di sicurezza".

Provvedimenti e Linee guida del Garante Privacy Italiano, in fase di armonizzazione:

- "Linee Guida per il trattamento di dati dei dipendenti privati" emesse il 23/11/2006;
- "Lavoro: linee guida per posta elettronica e Internet" emesse il 1° marzo 2007;
- Provvedimento in ordine all'applicabilità alle persone giuridiche del Codice in materia di protezione dei dati personali a seguito delle modifiche apportate dal d.l. n. 201/2011 emesso il 20 settembre 2012;
- Provvedimento in materia di videosorveglianza emesso l'8 aprile 2010;
- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema emesso il 27/11/2008;
- Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali.

2.2) Definizioni

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

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

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

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;

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

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «**destinatario**»: 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;

10) «**terzo**»: 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;

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;
12) «**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 o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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

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

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

16) «**stabilimento principale**»:
a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

23) «**trattamento transfrontaliero**»:
a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3) METODOLOGIA DI GESTIONE DELLA COMPLIANCE

3.1) Il sistema documentale

Operativamente il modello di conformità viene declinato attraverso l'implementazione del **SISTEMA DOCUMENTALE** di seguito descritto:

DOCUMENTO	RIF.LEGGE	DESCRIZIONE
Manuale Privacy_GDPR	Art.5, c.2	Il presente manuale è finalizzato a fornire evidenza del rispetto dei requisiti del GDPR
Autorizzazione Istruzioni	Art.29	Fascicolo con cui si autorizzano ed istruiscono i dipendenti ad un corretto e lecito trattamento dei dati acquisiti dall'organizzazione
Nomina Esterni	Art.28	Modulo da utilizzarsi per richiedere garanzie di tutela a tutti i soggetti esterni che trattano dati per conto dell'organizzazione
Nuovo Trattamento	Art.25	Format per le valutazioni preliminari da effettuarsi prima dell'inizio di nuove attività di trattamento
Registro Violazioni	Art.33	Format per la registrazione degli eventi che possono compromettere la sicurezza dei dati personali
Comunicazione Violazioni	Art.34	Format per la comunicazione dei data breach all'Autorità garante ed agli interessati
Informativa dipendenti	Art.13	Informazioni fornite al personale in merito al trattamento dei loro dati personali da parte dell'organizzazione
Informativa Web	Art.13	Ulteriori informazioni in merito alle privacy policy adottate dall'organizzazione
Diciture semplificate	Art.13	Eventuali modalità semplificate di informativa (es: inserimento in disclaimer email, documentazione di vendita, contrattualistica, ecc.
Diritti interessati	Art.15-21	Format per una corretta gestione delle richieste di esercizio dei diritti da parte degli interessati

3.2) Aggiornamento, distribuzione, validazione, divulgazione, validità

Il suddetto sistema documentale è gestito come segue.

Aggiornamento

- Il manuale privacy sarà oggetto di verifica ed aggiornamento su base annuale.
- Su base annuale sarà inoltre effettuato un audit di conformità complessivo, con verifica dei rating di rischio assegnati e validità del piano di sicurezza implementato.
- Gli allegati saranno oggetto di aggiornamento immediato in caso di variazioni significative dei contenuti.

Repository

- Tutti i documenti sono conservati in Originale presso la sede del Titolare
- Una copia conforme digitale è conservata presso sede della società incaricata (Data Protection Officer)

Validazione

La validazione del Titolare in calce al Manuale è da ritenersi estesa agli allegati citati in calce all'indice.

Divulgazione
Il Manuale e allegati sono divulgabili individualmente solo a soggetti direttamente coinvolti nel sistema, oppure a soggetti preposti a verifiche di legge (es: autorità ispettive, collegio sindacale). Su specifica e motivata richiesta saranno potranno essere portate a conoscenza di ulteriori soggetti interessati (eventualmente in forma semplificata/anonimizzata).

Validità
Ai sensi delle significative novità introdotte dal GDPR il Titolare ha deciso di effettuare una revisione complessiva della compliance privacy, pertanto il presente manuale e relativi allegati annullano e sostituiscono la documentazione precedentemente adottata (ci si riserva la facoltà di effettuare semplici integrazioni in merito alla documentazione già sottoscritta con gli incaricati / interessati, per esempio moduli di nomina ed informative).

Perimetro di applicazione
Il presente manuale si applica a tutti i trattamenti effettuati dall'organizzazione in qualità di Titolare.In particolare si applica ai trattamenti effettuati:

- presso le sedi territoriali;
- da personale autorizzato;
- attraverso strumenti elettronici forniti dall'organizzazione.

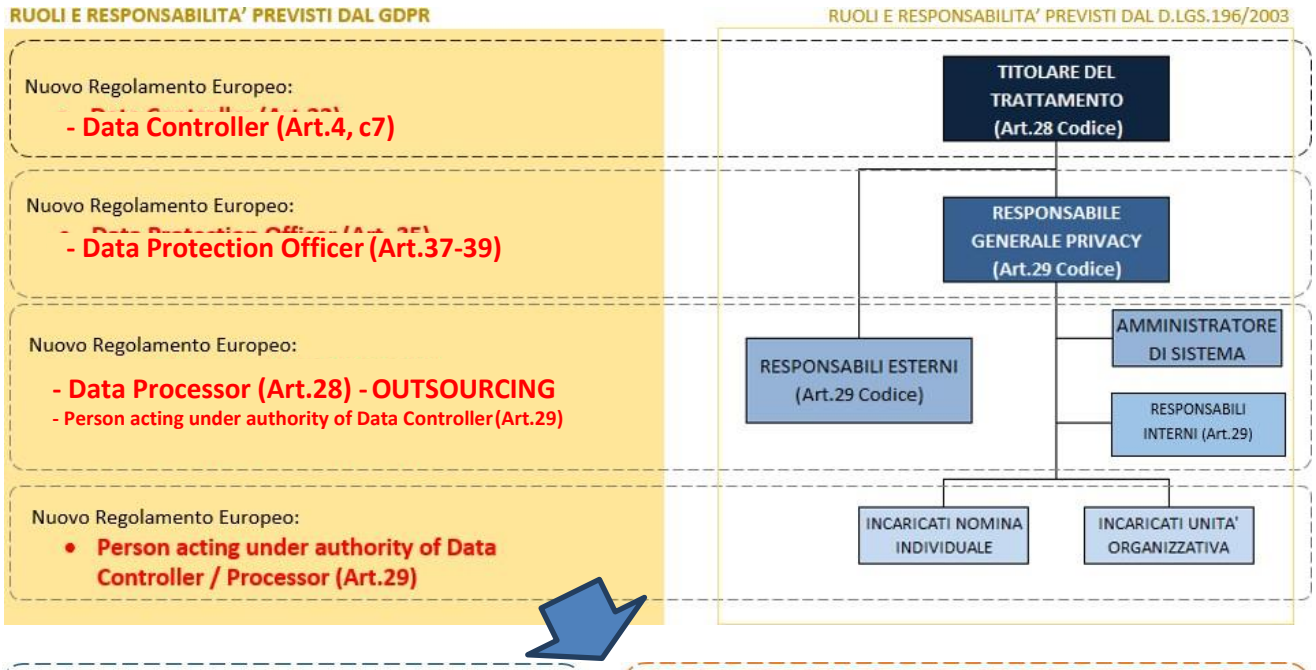
Altri possibili ruoli privacy
Qualora si venisse nominati Responsabili esterni da altro Titolare sarà cura dell'organizzazione valutare l'atto di designazione e rispettarne le eventuali specifiche istruzioni. Anche eventuali rapporti intercompany / rapporti di contitolarità del trattamento saranno gestiti secondo le specifiche necessità connesse al flusso di dati.

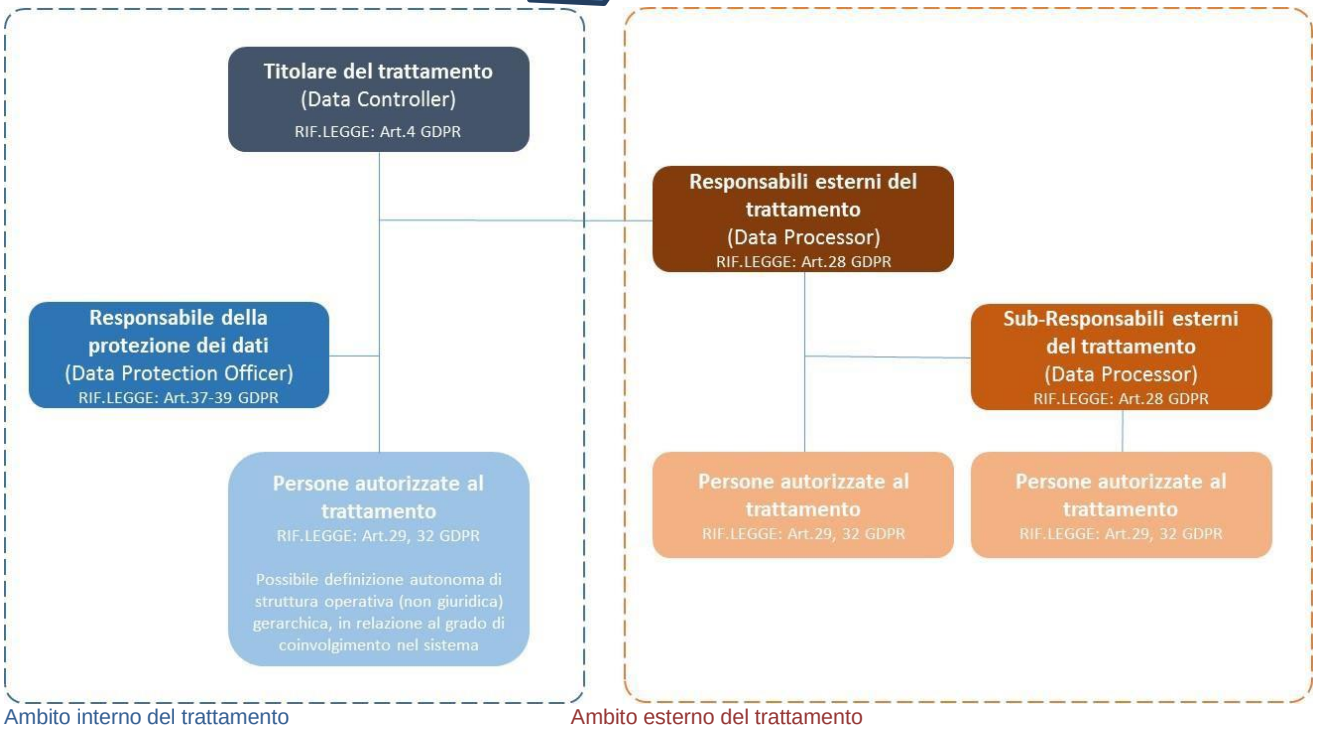
4) RUOLI E RESPONSABILITÀ PREVISTI DALLA NORMATIVA

Scopo del presente capitolo è **definire la distribuzione dei compiti e delle responsabilità** nell'ambito dei soggetti preposti al trattamento dei dati.

4.1 Riferimenti normativi

Il seguente organigramma definisce i ruoli previsti dal GDPR, effettuando un parallelo con i corrispettivi identificati dal D.Lgs.196/2003.





4.2 Assegnazione ruoli

Di seguito, in relazione al suddetto schema, vengono riportate le **scelte di governance** effettuate dall'organizzazione.

TITOLARE DEL TRATTAMENTO – DATA CONTROLLER

Definizione (Art.4, comma 7)

«Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

Responsabilità (Art.24)

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

IDENTIFICAZIONE:
L'entità giuridica dell'organizzazione, in persona del Legale Rappresentante

RESPONSABILI ESTERNI DEL TRATTAMENTO – DATA PROCESSOR

Definizione (Art.4, comma 8)

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Responsabilità (Art.28)

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

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

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..

IDENTIFICAZIONE:
Vedi atti di designazione allegati (2_ALL_Nomina Esterni)

PERSONE AUTORIZZATE AL TRATTAMENTO – PERSON AUTHORISED

Art.4, comma 10

«terzo»: 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

Articolo 29 Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

NOTA DI APPROFONDIMENTO:

Il GDPR non prevede espressamente la figura e la designazione dell' "incaricato del trattamento" (ex art. 30 D.Lgs.196/2003), ma fa esplicito riferimento a:

- "persone autorizzate al trattamento" (GDPR, Art.4, comma 10)
- "persone istruite al trattamento" (GDPR, Art.29)

Rientra pertanto nel concetto della "Responsabilizzazione del Titolare" le scelta delle modalità attuative con cui si ottempera ai suddetti requisiti (autorizzazione ed istruzione), anche in maniera differenziata rispetto all'organizzazione gerarchica del personale e rispettive mansioni.

IDENTIFICAZIONE:
Vedi autorizzazioni allegate (1_ALL_Autorizzazione Istruzioni)

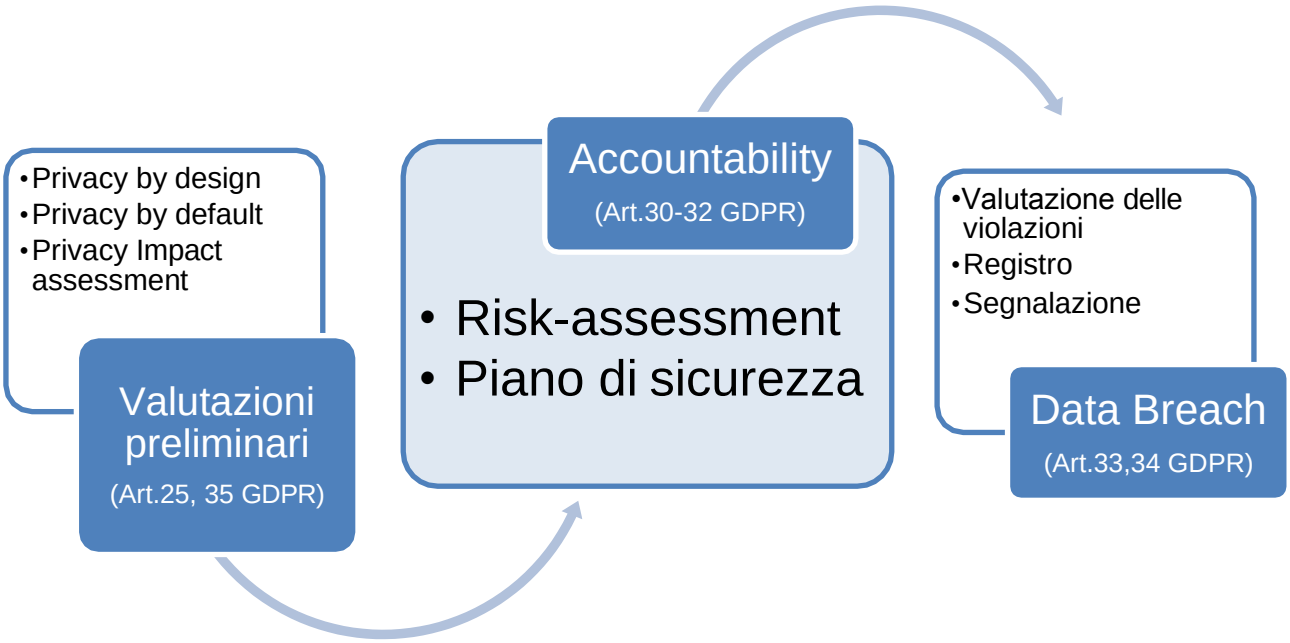
5) OBBLIGHI GENERALI DEL TITOLARE DEL TRATTAMENTO

Gli obblighi del Titolare del trattamento sono complessivamente definiti nel **Capo IV del GDPR** e sinteticamente riassunti nell'**Art.24**:

> *"1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*
> *2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento."*

Art.24 GDPR: Responsabilità del Titolare del trattamento

Il suddetto principio generale viene declinato in 3 fasi di compliance, secondo il seguente schema logico:



Il Titolare del trattamento è chiamato infine a effettuare specifiche valutazioni, nonchè implementare adeguate garanzie di tutela e protezione, nel caso di **trasferimento internazionale di dati**, verso Paesi non appartenenti alla Comunità Europea.

6) VALUTAZIONI PRELIMINARI ALLE ATTIVITÀ DI TRATTAMENTO

Al fine di poter dimostrare la conformità con il GDPR, il titolare del trattamento deve adottare politiche interne e attuare misure che soddisfino in particolare i principi della **protezione dei dati fin dalla progettazione** (Privacy by Design), della **protezione dei dati per impostazione predefinita** (Privacy by Default), nonché della **valutazione preliminare di impatto** (Privacy Impact Assessment).

Tali valutazioni devono essere effettuate:

- entro il 25 Maggio 2018 per i trattamenti già in essere (al fine di continuare lecitamente l'attività di trattamento ed inserire i dati nel registro dei trattamenti);
- in via antecedente all'inizio del trattamento per ogni futura attività.

6.1) Privacy by Design e Privacy by Default

La seguente tabella identifica le azioni effettuate al fine di garantire i requisiti di privacy fin dalla progettazione e privacy per impostazione predefinita:

RIF.LEGGE	OBBLIGHI	ATTUAZIONE		CRITERI DI VALUTAZIONE
		Trattamenti in essere al 25/05/2018	Nuovi trattamenti	
Privacy by Design *Art.25, comma1*	*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,* ***sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento*** *stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*	*Si è provveduto a verificare le misure di sicurezza in essere rispetto alla portata del trattamento ed ai requisiti del GDPR*	*Predisposto modulo per effettuare le medesime valutazioni anche per eventuali nuovi futuri trattamenti*	• *Misure tecniche e organizzative adeguate* • *Pseudonimizzazione* • *Minimizzazione*
Privacy by Default *Art. 25, comma 2*	*Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati,* ***per impostazione predefinita, solo i dati personali necessari*** *per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.*	*Si è provveduto a verificare la minimizzazione dell'utilizzo di dati, nonché la pertinenza*	*Predisposto modulo per effettuare le medesime valutazioni anche per eventuali nuovi futuri trattamenti*	• *Quantità di dati personali raccolti* • *Portata del trattamento* • *Periodo di conservazione* • *Accessibilità* • *Valutazione del life-cycle del dato*

6.2) Valutazione d'impatto sulla protezione dei dati (PIA, Privacy Impact Assessment)

Qualora, a seguito delle valutazioni di privacy by design e by default, emergano trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche occorre effettuare una **valutazione di impatto sulla protezione dei dati** (Privacy Impact Assessment, Art. 35 GDPR) per determinare l'origine, la natura, la particolarità e la gravità di tale rischio.

All'esito di questa valutazione di impatto si deciderà in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento. Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, ai quali il Titolare provvederà ad aggiornarsi.

ATTIVITA' DI TRATTAMENTO DA SOTTOPORRE A PIA

Il GDPR, all'interno dell'obbligo generale di condurre una PIA al ricorrere di un rischio elevato per gli interessati, fornisce alcune casistiche esemplificative (non esaustive) di trattamenti soggetti all'obbligo:

- 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;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

ELEMENTI DI ANALISI CHE DEVE CONTENERE LA PIA

- 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;
- 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.

6.3) Evidenze sule valutazioni preliminari alle attività di trattamento

In relazione al processo di adeguamento al GDPR sviluppato dal Titolare, **tutte le attività in essere al 25/05/2018 sono state analizzate secondo i requisiti di privacy by default, by design e PIA precedentemente elencati.** Al fine di presidiare tali requisiti anche per i **futuri trattamenti**, il Titolare ha predisposto una **scheda di analisi** attraverso la quale verranno valutati i requisiti di conformità in via antecedente all'inizio del trattamento.

7) IL PRINCIPIO DI ACCOUNTABILITY (RESPONSABILIZZAZIONE DEL TITOLARE)

Il GDPR pone con forza l'accento sulla "**responsabilizzazione**" (accountability nell'accezione inglese) del Titolare – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (Artt. 23-25, in particolare, e l'intero Capo IV del regolamento).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative ed in relazione ad una valutazione preliminare di rischio.

7.1) Valutazione del rischio

Nel GDPR la fase di valutazione del rischio si colloca al centro del processo di "Responsabilizzazione". Tale analisi è propedeutica ad implementare adeguate misure di sicurezza organizzative e tecniche, secondo quanto richiesto dall'Art.32.

Riferimenti normativi

ARTICOLI GDPR in cui si riporta la necessità di effettuare un'analisi di rischio:

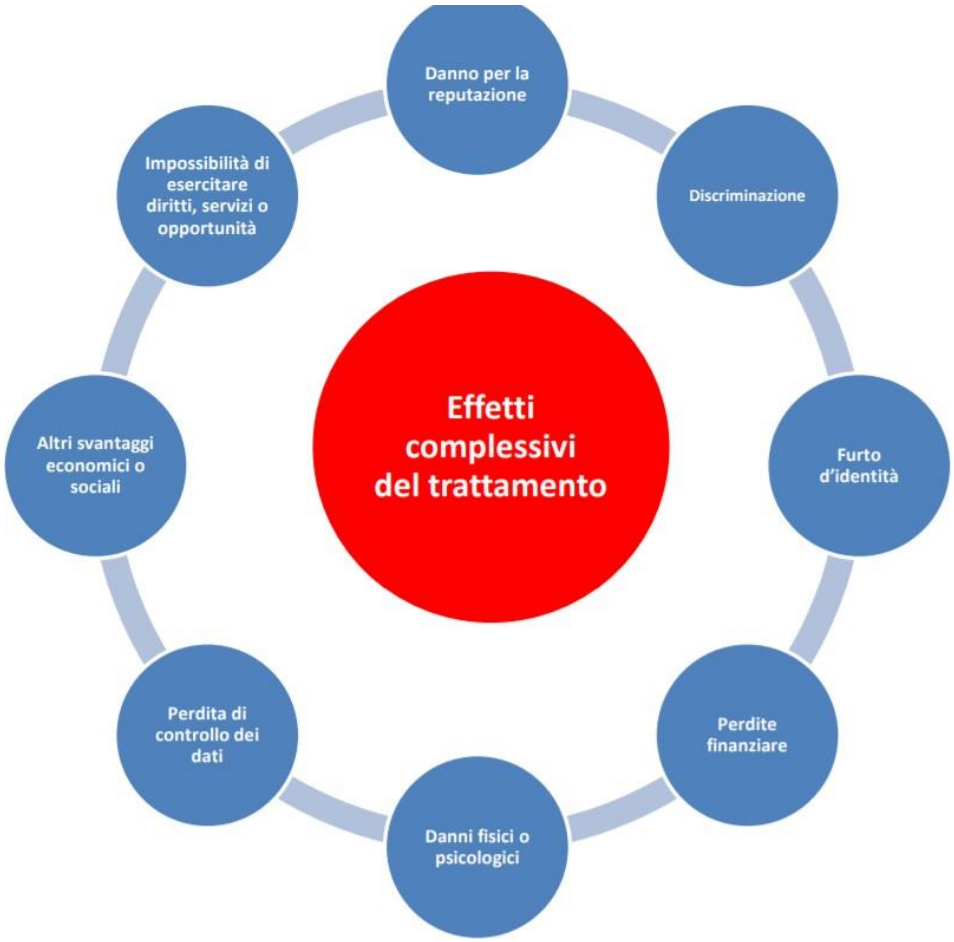
- *Art. 24 "Responsabilità del Titolare del trattamento"*
- *Art.25 "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Privacy by Design e by Default)*
- *Art.32 "Sicurezza del trattamento"*
- *Art. 33 "Notifica di una violazione di dati personali" (Data Breach)*
- *Art.34 "Comunicazione di una violazione di dati personali"*
- *Art.35 "Valutazione d'impatto sulla protezione dei dati" (Privacy Impact Assessment)*
- *Art.36 "Consultazione preventiva"*

CONSIDERANDO GDPR:

- *Considerando 75 "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."*
- *Considerando 76 "La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.*
- *Considerando 83 "Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.*

Metodologia (considerazioni preliminari)

L'attività di trattamento dati personali è considerata dal legislatore quale "attività rischiosa", poiché può comportare delle conseguenze negative nei confronti di coloro che hanno conferito tali dati. Il seguente schema effettua una classificazione delle principali tipologie di tali conseguenze negative.



Pertanto, preliminarmente alla definizione della metodologia occorre focalizzare il **vero obiettivo dell'analisi di rischio** prevista dal GDPR, ossia l'impatto sui diritti e le libertà fondamentali delle persone fisiche. Il legislatore focalizza dunque il processo sull'interessato, invitando a sensibilizzare il Titolare sulle possibile conseguenze che i trattamenti effettuati possano generare sulle persone che hanno conferito tali dati (interessati).

In particolare occorre identificare una **metodologia che definisca quale livello di rischio per gli interessati possa derivare da un evento dannoso quale distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzato**.

Elementi da considerare nella individuazione del rischio
(vedi tutorial del Garante pubblicato in data 27/04/2018
http://www.garanteprivacy.it/regolamentoue/dpia/gestione-del-rischio)

LEGENDA DEL LIVELLO COMPLESSIVO DI RISCHIO:

1 RISCHIO TRASCURABILE

2 RISCHIO LIMITATO

3 RISCHIO SIGNIFICATIVO

4 RISCHIO IMPORTANTE

5 RISCHIO CRITICO

In relazione al contesto operativo del Titolare, all'origine e natura dei dati trattati, alla gravità delle conseguenze di un evento dannoso, alla probabilità di accadimento di tale evento, all'impatto sui diritti e le libertà delle perone fisiche di cui il Titolare tratta dati personali, il livello complessivo di rischio è stimato in:

- RISCHIO LIMITATO

7.2 Piano di sicurezza

Nel GDPR l'implementazione di adeguate misure di sicurezza a tutela dei dati si colloca alla fine del processo di "responsabilizzazione". Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio (art.32, par.1). Per tale motivo il GDPR fornisce una lista aperta non esaustiva. Per lo stesso motivo non possono sussistere dopo il 25/05/2018 obblighi generalizzati di adozione di "misure minime" di sicurezza, poiché tale valutazione è rimessa, caso per caso, al Titolare, in rapporto ai rischi specificatamente individuati.

Riferimenti normativi

Art. 32 "Sicurezza del trattamento"
1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
Art.24 "Obblighi generali"
1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Il titolare attualmente riassume nella seguente tabella le aree e le misure di sicurezza implementate per una corretta gestione del rischio privacy indiciduato.

TIPOLOGIA	MISURE	STATO	NOTE
Misure tecnologiche	Policy di autenticazione ed autorizzazione utenti	IN ESSERE	Misure in essere e soggette a monitoraggio periodico
	Sistemi difesa malware	IN ESSERE	
	Sistemi difesa perimetrale	IN ESSERE	
	Sistemi back-up e recovery	IN ESSERE	
Misure organizzative	Segregazione ruoli e permessi	IN ESSERE	Misure in essere e soggette a monitoraggio periodico
	Autorizzazione, istruzioni, consapevolezza, formazione, regolamenti	IN ESSERE	
	Procedure di controllo ed aggiornamento	IN ESSERE	
	Tutela della sicurezza fisica di sede, locali ed archivi	IN ESSERE	
	Procedure a garanzia degli interessati (informazioni e diritti)	IN ESSERE	

8) GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

IL GDPR prevede l'obbligo, per tutti i Titolari, di notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (GDPR, considerando 85). Il Titolare provvede in ogni caso a documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

8.1 La definizione e le tipologie di Data Breach

Si ha una "**violazione dei dati personali**" quando accidentalmente (colposamente) o in modo illecito (dolosamente) un evento causa la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati personali trasmessi, conservati o comunque trattati. Nelle tabelle seguenti sono riportati alcuni esempi a cui è associato l'impatto prevalente sulle proprietà di sicurezza delle informazioni comunemente espresse in termini di Riservatezza (R), Integrità (I) e Disponibilità (D).

1. DISTRUZIONE:	**Indisponibilità irreversibile dei dati personali con appurata impossibilità di ripristino degli stessi**		
Accidentale	La distruzione dei dati personali può essere causata da un evento naturale al di fuori del controllo umano (allagamento, incendio, terremoto, ecc.) oppure da malfunzionamenti tecnici che provocano danni irreparabili alle infrastrutture informatiche oppure ai dati conservati nelle apparecchiature (server, PC, laptop dispositivi mobili, media, ecc.)		
Illecita	La distruzione dei dati personali può derivare da instabilità sociale (terrorismo, guerra, proteste ecc.) oppure da eventi deliberati (danneggiamento fisico o manomissione di infrastrutture informatiche, apparecchiature, ecc.)		
Proprietà di sicurezza	**R**	**I**	**D**

2. PERDITA:	**Smarrimento o sottrazione dei dati personali**		
Accidentale	La perdita dei dati personali può originare dallo smarrimento di apparecchiature (server, PC laptop, dispositivi mobili, media, ecc.), oppure dallo smaltimento non sicuro dei supporti di archiviazione dei dati (hard disk, media, ecc.), da un errori umani che compromettono la funzionalità del sistema corrompendo gli archivi di memorizzazione dei dati oppure che inavvertitamente effettuino una cancellazione sicura dei dati con appurata impossibilità di ripristino degli stessi		
Illecita	La perdita dei dati personali può essere determinata dal furto di apparecchiature (server, workstation, laptop, dispositivi mobili, media, ecc.), da eventi deliberati tesi alla cancellazione sicura dei dati con appurata impossibilità di ripristino degli stessi		
Proprietà di sicurezza	**R**	**I**	**D**

3. MODIFICA:	**Cambiamento di dati personali improprio o non autorizzato in grado di compromette la completezza e/o la correttezza delle informazioni**		
Accidentale	La modifica di dati personali può essere causata da errori umani in grado di apportare cambiamenti indesiderati alle informazioni contenuti in banche dati		
Illecita	La modifica di dati personali può derivare dall'azione di malware		
Proprietà di sicurezza	**R**	**I**	**D**

4. DIVULGAZIONE NON AUTORIZZATA:	**Rivelazione di dati personali a soggetti terzi determinati o indeterminati**		
Accidentale	La divulgazione non autorizzata dei dati personali è causata da un errore umano che espone impropriamente dati personali a terzi (es. invio via email di documenti a destinatari errati)		
Illecita	La divulgazione non autorizzata dei dati personali avviene deliberatamente da parte di criminali informatici che espongono le informazioni personali online a seguito di un accesso abusivo		
Proprietà di sicurezza	**R**	**I**	**D**

5. ACCESSO NON AUTORIZZATO	**Compimento di operazioni di trattamento da parte di soggetti non autorizzati**		
Accidentale	Errata configurazione dei sistemi che permette a soggetti non autorizzati di compiere operazioni sui dati		
Illecita	Attività di spionaggio attraverso l'uso di dispositivi hardware (es. keylogger) e software (intercettazione del traffico di rete, trojan, ecc.) Attacco alle applicazioni web per sfruttare vulnerabilità e ottenere l'accesso ai sistemi		
Proprietà di sicurezza	**R**	**I**	**D**

8.2 Gli obblighi previsti dal GDPR

Gli obblighi normativi associati a violazioni di dati personali sono riportati dagli artt. 33 e 34 del GDPR

Articolo 33 "Notifica di una violazione dei dati personali all'autorità di controllo"	**Articolo 34 "Comunicazione di una violazione dei dati personali all'interessato"**
1. In caso di violazione dei dati personali, il titolare del trattamento **notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. 3. La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. 4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.	1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento **comunica la violazione all'interessato** senza ingiustificato ritardo. 2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). 3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. 4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Il titolare del trattamento **documenta qualsiasi violazione dei dati personali**, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

9. FONDAMENTI DI LICEITÀ DEI TRATTAMENTI

Il GDPR specifica che ogni trattamento deve **trovare fondamento in un'idonea base giuridica**. Pertanto, ogni attività di trattamento, per potersi considerare lecita, deve trovare un riscontro in uno o più tra i**fondamenti di liceità** indicati all'art. 6 del regolamento:

a) l'interessato ha espresso il **CONSENSO AL TRATTAMENTO** dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'**ESECUZIONE DI UN CONTRATTO** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un **OBBLIGO LEGALE** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la **SALVAGUARDIA DEGLI INTERESSI VITALI** dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un **COMPITO DI INTERESSE PUBBLICO** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del **LEGITTIMO INTERESSE** del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, in particolare se l'interessato è un minore.

I seguenti paragrafi approfondiscono i suddetti principi di liceità, evidenziando ulteriori elementi utili a definirne l'applicabilità ai trattamenti effettuati dal Titolare.

9.1) Trattamento basato sul consenso dell'interessato

E' da intendersi come «consenso dell'interessato» qualsiasi manifestazione di volontà libera, specifica,informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprioassenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali chelo riguardano siano oggetto di trattamento. L'istituto del consenso è subordinato alle condizioni identificate nella seguente tabella.

Rif.Legge	Condizioni per il consenso
GDPR, Art. 7, comma 1 **Dimostrabilità**	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.
GDPR, Art. 7, comma 2 **Forma**	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.
GDPR, Art. 7, comma 3 **Revocabilità**	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 esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
GDPR, Art. 7, comma 4 **Libertà**	Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Rif.Legge	Condizioni per il consenso
GDPR, Art. 8 **Consenso di minori**	Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
GDPR, Art.9 **Categorie particolari di dati personali**	In generale è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Tale divieto non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio **consenso <u>esplicito</u> al trattamento** di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare 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 in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

9.2) Trattamento necessario all'esecuzione di un contratto con l'interessato

Il trattamento è considerato lecito se è necessario nell'ambito di uncontratto o ai fini della conclusione di un contratto con l'interessato o per misure precontrattuali adottate su richiesta dell'interessato stesso.

9.3) Trattamento necessario ad adempiere ad un obbligo legale

È opportuno che il trattamento effettuato in conformità a un obbligo legale al qualeil titolare del trattamento è soggettosia basato sul dirittodell'Unione o di uno Stato membro. Il GDPR non impone che vi siaun atto legislativo specifico per ogni singolo trattamento. Un atto legislativo puòessere sufficiente come base per più trattamenti effettuati conformemente a un obbligolegale cui è soggetto il titolare del trattamento.

9.4) Trattamento necessario per la salvaguardia di interessi vitali

Il trattamento di dati personali è altresì considerato lecito quando ènecessario per proteggere un interesse essenziale per la vita dell'interessato o diun'altra persona fisica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motividi interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamentoè necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzionedi epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolarein casi di catastrofi di origine naturale e umana. In relazione alla tipologia di attività esercitata dal Titolare (*vedi SGP_POL_Politica, Cap.5 "Analisi di contesto"*) non vengono di norma effettuati trattamenti di dati personali sulla base del presente principio di liceità.

9.5) Trattamento connesso all'esercizio di pubblici poteri

Il Titolare del trattamento non è un organismo pubblico, pertanto non vengono effettuati trattamenti di dati personali sulla base del presente principio di liceità.

9.6) Trattamento connesso al perseguimento di un legittimo interesse del Titolare

I legittimi interessi delTitolare del trattamento possonocostituire una base giuridica del trattamento, a condizione che non prevalgano gliinteressi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delleragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolaredel trattamento (ad esempio, potrebbero sussistere tali legittimi interessi quandoesista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento,ad esempio quando l'interessato è un cliente o è alle dipendenze del titolaredel trattamento). In ogni caso, per valutare l'esistenza di legittimi interessi viene effettuata un'attentavalutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambitodella raccolta dei dati personali, possa ragionevolmente attendersi che abbialuogo un trattamento a tal fine.
La seguente tabella classifica alcune casistiche esemplificative in cui può ritenersi valido quale principio di liceità del trattamento un legittimo interesse del Titolare.

Rif.Legge	Descrizione legittimo interesse
GDPR, C.47 **Autotutela**	Può essere considerato legittimo effettuare attività di trattamento ai fini di **tutela del patrimonio, sicurezza, prevenzione frodi, acquisizione prove, diritto di difesa** (es. videosorveglianza)
GDPR, C.47 **Marketing**	Può essere considerato legittimo interesse trattare dati personali per finalità di **marketing diretto**
GDPR, C.47 **Flussi intercompany**	I titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo a **trasmettere dati personali all'interno del gruppo imprenditoriale** a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo.
GDPR, C.47 **Dati di traffico**	Costituisce legittimo interesse del titolare del trattamento trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi.Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.

10. IL PRINCIPIO GENERALE DELLA TRASPARENZA E GLI ATTI DI INFORMAZIONE

Già nel Codice della Privacy (D.Lgs. 196/2003) l'informativa all'interessato rappresentava uno degli adempimenti principali in capo al titolare del trattamento, sia esso un soggetto privato sia esso un soggetto pubblico. Per quanto già il singolo adempimento "informativa" giochi un ruolo determinante nello sviluppo di una equilibrata relazione tra titolare e interessato, va evidenziato come tale singolo adempimento si inserisca nel più vasto contesto del "principio di trasparenza".Nello studio evolutivo, dal Codice della Privacy al Regolamento Ue 2016/67, occorre immediatamente evidenziare la maggiore significatività del principio generale della"trasparenza", con tutte le conseguenze che ne derivano.

L'articolo 5, paragrafo 1, lettera a) del Regolamento 2016/679, prescrive che idati personali siano trattati "in modo trasparente nei confronti dell'interessato".

La prescrizione generale della trasparenza è elemento costitutivo fondamentale della "responsabilizzazione" e la prova dell'adeguamento dei trattamenti è tutta a carico del titolare (art. 5 citato).

La portata del principio generale, inoltre, è determinata dalla qualità e quantità del connesso profilo sanzionatorio. La prescrizione della trasparenza, a questo proposito, al netto delle conseguenze civili(risarcimento del danno), è assistita dalla sanzione amministrativa disciplinata dal paragrafo3 dell'articolo 83, che è la più pesante in termini edittali (fino a € 20mln o 4% del fatturato mondiale consolidato).Mancare di trasparenza espone a tale conseguenza, oltre che ai poteri di indagine e agliinterventi correttivi dell'Autorità di controllo (art. 58 del Regolamento).

Il Titolare prevede pertanto un **approccio consapevole e sistematico ai requisiti di trasparenza**, garantendone l'attuazione e la conoscibilità attraverso:

- servizi di fornitura di informazioni all'interessato prima e nel corso dei trattamenti, mediante canali (anche multimediali) che assicurino un accesso agevole e capillare;
- disclosure sull'identità dei soggetti che, a vario titolo, trattano i dati personali e sulle strutture di riferimento da contattare per assistenza in materia di privacy;
- disclosure sui mezzi utilizzati per il trattamento e da utilizzare per esercitare richieste o diritti.

10.1 La trasparenza come diritto

Il principio generale "trasparenza" viene dettagliato dal Regolamento nella parte dedicata ai"diritti" (capo III) e si sdoppia in "diritto alla trasparenza"(art. 12) ed "informazioni" (articoli 13 e 14).L'istituto specifico del "diritto alla trasparenza" (art. 12), concettualmente distinto dal"principio generale della trasparenza" (Art.5),definisce le modalità secondo cui il Titolare del trattamento deve fornire:

- le informazioni di cui agli artt.13-14 (informative sul trattamento dei dati)
- le comunicazioni di cui agli artt.15-23 (diritti degli interessati)

La seguente tabella classifica le modalità, previste dal GDPR, per garantire il diritto alla trasparenza.

Forma delle comunicazioni	Il Titolare adotta misure appropriate per fornire all'interessato tutte le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici; se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

Obbligo di riscontro	Il Titolare agevolare l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento **non può rifiutare di soddisfare la richiesta dell'interessato** al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato
Tempistiche del riscontro	Il Titolare fornisce all'interessato i riscontri richiesti ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.
Casi di inottemperanza	Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
Compenso per i riscontri	Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 **sono gratuite**. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può: a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure b) rifiutare di soddisfare la richiesta (incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta).
Richiesta di approfondimenti	Qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

10.2 Le informazioni da fornire agli interessati

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13 e 14 del GDPR, risultando in parte differenti rispetto al D.Lgs.196/2003. Gli articoli 13 e 14 del GDPR sono dedicati rispettivamente alle informazioni da fornire "qualora i dati personali siano raccolti presso l'interessato" e alle informazioni da fornire "qualora i dati personali non siano ottenuti presso l'interessato" (vedi seguente tabella).

	Dati raccolti presso l'interessato (GDPR, Art.13)	**Dati non ottenuti presso l'interessato (GDPR, Art.14)**
CONTENUTI	• l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; • i dati di contatto del responsabile della protezione dei dati, ove applicabile; • le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; • qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; • gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; • ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili. • il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; • l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; • l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; • il diritto di proporre reclamo a un'autorità di controllo; • 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; • l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.	• l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; • i dati di contatto del responsabile della protezione dei dati, ove applicabile; • le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; • le categorie di dati personali in questione; • gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; • ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili. • il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; • qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; • l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; • qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; • il diritto di proporre reclamo a un'autorità di controllo; • la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; • l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
TEMPI	Nel momento in cui i dati sono ottenuti	• entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; • nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure • nel caso sia prevista la comunicazione ad altro

	Dati raccolti presso l'interessato (GDPR, Art.13)	Dati non ottenuti presso l'interessato (GDPR, Art.14)
		destinatario, non oltre la prima comunicazione dei dati personali
TRATTAMENTO PER FINALITA' DIVERSE	Qualora si intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento si fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.	Qualora si intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento si fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente.
CASI DI ESONERO	Gli obblighi dell'informativa non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.	Gli obblighi dell'informativa non si applicano se e nella misura in cui: • l'interessato dispone già delle informazioni; • comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni; • l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure • qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

In riferimento alle attività di trattamento effettuate dall'organizzazione ed alle categorie di interessati di cui si acquisiscono dati, si sono attualmente predisposte le seguenti informative:

- Informativa dipendenti
- Informativa Web

11. I DIRITTI DEGLI INTERESSATI

Il GDPR, per quanto concerne il tema dei "diritti" degli interessati al trattamento, presenta diversi elementi di continuità con la normativa del recente passato (D.Lgs. 196/2003 e Direttiva 95/46/CE); il legislatore europeo ha tuttavia introdotto (nella lunga elencazione che va dall'art. 15 al 22 del GDPR) **nuove prerogative riconosciute agli interessati al trattamento**, tenendo in considerazione l'attuale sviluppo delle nuove tecnologie che potenzialmente possono determinare nuovi pericoli e rischi per i diritti e le libertà degli stessi.Di seguito viene riportata un'elencazione dei diritti degli interessati previsti dal GDPR (par.3.1), nonché le modalità attuative implementate dal Titolare per fornire un puntuale ed esaustivo riscontro ad eventuali richieste degli interessati (par. 3.2).

11.1) Classificazione dei diritti degli interessati

La seguente tabella riporta un elenco dei diritti degli interessati previsti dal GDPR, recepiti dal Titolare e garantiti dal DPO attraverso apposita procedura e specifici allegati.

Diritto	Descrizione
ART.15 **Diritto di accesso**	L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.
ART.16 **Diritto di rettifica**	L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
ART.17 **Diritto di cancellazione (oblio)**	L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Esclusioni: i suddetti diritti non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione;

Diritto	Descrizione
	b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
ART.18 **Diritto di limitazione**	L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
ART.20 **Diritto alla portabilità dei dati**	L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b)il trattamento sia effettuato con mezzi automatizzati. Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il diritto di cui alla portabilità non deve ledere i diritti e le libertà altrui.
ART.21 **Diritto di opposizione**	L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
ART.22 **Processi decisionali automatizzati (profilazione)**	L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Il suddetto paragrafo non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

12) TRASFERIMENTO INTERNAZIONALE DI DATI

Il GDPR ha confermato l'approccio vigente in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i **flussi di dati al di fuori dell'Unione europea** e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

- adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;
- in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello);
- in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

Le decisioni di adeguatezza sinora adottate dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica.

Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione (si veda http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi).

Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi, sino a loro eventuale modifica.

Evidenze sul trasferimento internazionale di dati

Qualora si dovesse riscontrare l'esigenza di un trasferimento di dati all'estero (extra UE), sarà verificato quale dei seguenti requisiti di liceità adottare come riferimento:

- Trasferimento Extra UE - Paesi adeguati
- Trasferimento Extra UE - Clausole contrattuali
- Trasferimento Extra UE - Norme vincolanti gruppo.