G.D.P.R.

GENERAL DATA PROTECTION REGULATON

REGOLAMENTO UE 679/2016

CHANGE+
CONSULENZA AZIENDALE

ESTRATTO del REGOLAMENTO per gli iscritti alla NEWSLETTER di www.changeplus.it e per i partecipanti agli eventi CHANGE+ S.r.l.

P.le Gerbetto 6
22100 Como (CO)
Partita I.V.A. e Codice Fiscale: 02850040128

Sommario

1. Che cosa è?

G.D.P.R. è l'acronimo di General Data Protection Regulation, ovvero il Regolamento generale sulla protezione dei dati personali vigente nell'Unione Europea. Pubblicato in data 4 Maggio 2016, ha l'ambizione di rafforzare ed unificare la normativa sulla protezione dei dati personali entro i confini UE, superando i parziali regolamenti locali oltre a regolare anche il tema dell'esportazione dei dati al di fuori dei confini UE. È in vigore dal 25 Maggio 2018 e ha abrogato il D. Lgs. 196/03 "Codice Privacy".

2. Gli ambiti di applicazione

La riforma introdotta dal G.D.P.R. impatta, tecnicamente, sulla protezione, elaborazione e circolazione dei dati personali. Essa interessa tutte le imprese, i professionisti e gli enti che trattano i dati personali di persone fisiche.

Sono esclusi i trattamenti di dati effettuati da persone fisiche nell'esercizio di attività a carattere esclusivamente personale o domestico, nonché quelli a cura di autorità competenti con finalità di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali.

Dal punto di vista territoriale, il G.D.P.R. riguarda il trattamento dei dati personali eseguito nell'ambito delle attività poste in essere all'interno dell'Unione Europea, anche qualora il trattamento avvenga al di fuori della stessa. Si applica, inoltre, al trattamento dei dati personali di Interessati che non siano stabiliti nell'Unione Europea, quando lo stesso riguardi l'offerta di beni o la prestazione di servizi inerenti il territorio considerato, come anche il relativo monitoraggio.

Inoltre, riguarda anche il trattamento effettuato dal Titolare non stabilito nell'Unione, ma all'interno di un luogo comunque soggetto, in virtù del diritto internazionale, alla legislazione di uno Stato membro.

3. I diritti

Con il G.D.P.R., i diritti degli individui e riferiti alla protezione dei dati in generale, vengono rafforzati. Questo si traduce nella possibilità di accedervi più facilmente, nel conoscere in modo più approfondito le modalità di processo, trasferimento e gestione in genere. Oltre a questo, gli Interessati possono esigere la cancellazione (diritto di oblio) di quei dati di cui si dimostri non esista oltre motivo di conservazione.

4. La vigilanza e il rispetto

Il G.D.P.R. prevede una normativa unica per l'Unione Europea (valevole anche per le imprese extra-UE che offrano servizi nell'Unione Europea) e una sola Autorità (europea) di vigilanza. Le sanzioni sono note: fino a 20 Milioni di Euro e fino al 4% del fatturato prodotto dall'azienda a livello mondiale.

5. Come adeguarsi

L'adeguamento si compone di una serie di misure esemplificativamente riferibili a: mappatura dei dati personali, gestione dei rischi; governo dei dati (policy), individuazione di collegamenti tra processi e controllo delle procedure, management delle responsabilità, adozione di strategie di protezione, permission e misure per la cyber security, reportistica interna, censimenti, verifiche, conduzione del rapporto con gli interessati e denuncia delle violazioni.

6. L'approccio risk based e le misure di accountability

Il Regolamento pone con forza l'accento sul concetto di "responsabilizzazione", "accountability" nell'accezione inglese, di Titolari e Responsabili – vale a dire sull'**adozione di comportamenti proattivi atti a dimostrare la concreta adozione di misure che ne assicurino l'applicazione** *(si vedano 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 ai Titolari viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"** *(art. 25)*, ad indicare l'indispensabilità di configurare il trattamento prevedendo fin dalla progettazione l'adozione di tutte le garanzie che soddisfino i requisiti del Regolamento, a tutela degli Interessati e tenendo conto del contesto complessivo nel quale il trattamento si colloca e dei rischi associati ai diritti e alle libertà degli stessi. Tutto questo è quindi necessariamente da concepire già "a monte", vale a dire già in fase di progettazione, "sia nel momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 (1). Si richiedono, quindi, un'analisi preventiva ed un impegno applicativo da parte dei Titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

Fondamentali, fra tali attività, sono quelle connesse al secondo criterio individuato nel Regolamento a riferirsi alla gestione degli obblighi da parte dei Titolari, ossia al **rischio inerente il trattamento**. Quest'ultimo è da intendersi come rischio di impatti negativi sulla libertà e sui diritti degli interessati *(si vedano artt. 75-77)*; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione *(si vedano artt. 35-36)* tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati pubblicate dal Gruppo "Articolo 29". All'esito di questa valutazione di impatto, il Titolare potrà decidere in autonomia se dare corso al 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 eventuali misure ulteriormente implementabili a cura del Titolare; l'autorità potrà altresì, 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 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) che risultano ora 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" (l'erede dell'attuale Gruppo "Articolo 29") spetta un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi ed analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

INFORMATIVA:

CONFRONTO con la normativa precedente

Ex Art. 13 D. Lgs. 196/03	Artt. 12-22 REGOLAMENTO 679/2016

In quale momento devono essere adempiuti gli obblighi riferiti all'informativa?

L'informativa è un obbligo generale che va adempiuto prima o, al più tardi, al momento di dare avvio alla raccolta dei dati finalizzati al trattamento. Occorre ricordare che l'obbligo non ricorre: + quando il trattamento concerne dati che non sono personali, bensì anonimi (ad esempio, dati aggregati o statistici); + quando il trattamento riguarda i dati di Enti/ persone giuridiche: la normativa a protezione dei dati personali non concerne le informazioni relative a soggetti diversi dalle persone fisiche.	Vale integralmente quanto riportato nel Codice Privacy.

Quali soggetti non sono tenuti all'obbligo dell'informativa?

Non deve prestare l'informativa: + la persona fisica che effettui il trattamento per fini esclusivamente personali e laddove i dati non siano siano destinati alla comunicazione sistematica, ovvero alla diffusione; + il Titolare che riceva un *curriculum vitae* spontaneamente trasmesso dall'interessato, almeno fino al momento del primo contatto successive, laddove sarà da rendere una informativa specifica.	Non è tenuta a prestare l'informativa la persona fisica che effettui il trattamento dei dati per attività a carattere esclusivamente personale e domestico. Fino a pronunce diverse, restano validi i provvedimenti specifici di settore o di casistiche poste al Garante Privacy.

Resa dell'informativa per dati raccolti presso l'interessato e presso terzi

Nel caso di raccolta dei dati presso un terzo, l'informativa è fornita all'interessato:

+ nel momento in cui i dati sono registrati;
+ al momento della prima comunicazione, quando prevista.

L'informativa deve comprendere, oltre alle informazioni richieste in generale, anche l'indicazione delle categorie di quanto oggetto del trattamento (solo dati personali comuni o anche dati sensibili e/o giudiziari).

Nel caso di raccolta dei dati presso un terzo, l'informativa è fornita all'interessato:

+ entro un termine "ragionevole" e, comunque, non oltre un mese;
+ al momento della prima comunicazione, quando prevista.

L'informativa deve essere completa dei contenuti prescritti in via generale, con le seguenti aggiunte/differenze:

l'indicazione delle categorie dei dati personali oggetto del trattamento;
l'indicazione della fonte da cui hanno origine i dati personali;
la base giuridica del trattamento.

Si omette l'informazione circa la natura obbligatoria o meno della comunicazione di dati personali, perché nella fattispecie i dati non sono raccolti presso l'interessato.

Nel caso di raccolta presso terzi il titolare è sempre tenuto ad informare l'interessato?

Il Codice Privacy individua tre fattispecie nelle quali il titolare non è tenuto a informare l'interessato, vale a dire:

+ il trattamento è da eseguire in base ad un obbligo di Legge o di Regolamento, ovvero considerazione ad una norma comunitaria;
+ i dati sono da trattare ai fini dello svolgimento di investigazioni defensive, ovvero per far valere/difendere un diritto in sede giudiziaria;
+ l'informativa comporti un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, sempre per il Garante, impossibile.

Il Regolamento UE individua le fattispecie in cui il Titolare non è tenuto a informare l'interessato, quando:

+ l'interessato disponga già delle informazioni;
+ comunicare tali informazioni risulti impossibile o implichi uno sforzo sproporzionato;
+ l'ottenimento o la comunicazione siano espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare;
+ i dati personali debbano rimanere riservati per obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri.

L’informativa è da rendere in forma scritta o orale?

Sono forme parimenti ammesse dalla Legge ma è chiaro che una informativa scritta (riportata su supporto cartaceo e/o digitale, inviata e/o consegnata al destinatario con evidenza della ricezione da parte del medesimo) costituisca prova obiettiva dell’assolvimento dell’obbligo da parte del Titolare.

L’informativa deve essere resa per iscritto o con altri mezzi (anche elettronici, come, per es., la posta elettronica). Ove richiesto dall’interessato, l’informativa è da rendere oralmente (purché sia comprovata con altri mezzi l’identità dell’interessato).

Come previsto nel Codice Privacy, anche qui può essere opportuno che il Titolare si procuri e conservi una evidenza del rilascio dell’informativa.

7. Data Breach

Definizione Ex Art. 13 D. Lgs. 196/03	*Violazione della sicurezza che comporta, anche accidentalmente, la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.*
Artt. 12-22 REGOLAMENTO 679/2016	*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":*

In questo modo, **il G.D.P.R. ha amplificato notevolmente il significato in uso di violazione del dato, usualmente associato al solo furto.**

Secondo il G.D.P.R. le violazioni possono essere, infatti, di tre tipi:

1) **di confidenzialità**, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2) **di integrità**, quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3) **di disponibilità/accesso**, quando si verifica perdita, inaccessibilità, o distruzione, sempre non autorizzata o accidentale, di dati personali.

In uno qualsiasi di questi tre scenari, compito di accertare il data breach è del Titolare, o se presente, anche del Responsabile, il quale ha l'obbligo di avvisare tempestivamente il Titolare stesso.

Per il Data Breach è definito un iter ben preciso:

L'articolo 33 del Regolamento impone ad ogni società l'obbligo di notificare all'autorità nazionale (nel nostro caso il Garante per la Privacy), ENTRO 72 ORE, qualsiasi violazione di sicurezza che comporti la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali, indipendentemente dalla causa che l'ha generata.

Tale notifica deve:

1. descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione;
2. comunicare il nome e i dati di contatto del Responsabile della protezione dei dati o altro riferimento presso il quale ottenere più informazioni;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. 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.

Nel caso in cui la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e per le libertà fondamentali degli interessati, il Regolamento obbliga il Titolare del trattamento a comunicare tale violazione anche a ciascun Interessato al fine di consentirgli di adottare idonee precauzioni volte a ridurre al minimo il potenziale danno.
Tuttavia, si può essere esonerati dalla notifica all'interessato, laddove:

a) il Titolare del trattamento abbia messo in atto adeguate misure tecniche e organizzative di protezione e tali misure siano state applicate ai dati personali oggetto della violazione;

b) il Titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e per le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richieda sforzi sproporzionati. In tale caso, si procede invece ad una comunicazione pubblica o all'adozione di una misura simile, tramite la quale gli Interessati siano informati con analoga efficacia.

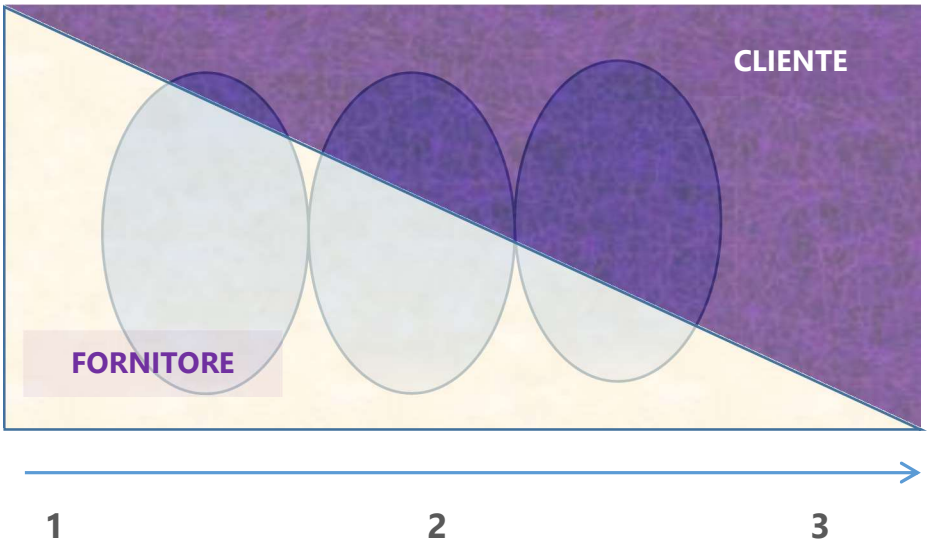
d) i contenuti delle comunicazioni violate siano interamente cifrati.

L'ipotesi d), tuttavia, è avveniristica poiché la cifratura completa dei dati mette a dura prova l'operatività aziendale, mentre la c) è demandata alla valutazione ex post di un giudice. Rimane, quindi, da capire quali siano le misure idonee atte a scongiurare il rischio. Il Regolamento 679/2916 viene in supporto stabilendo che "l'adesione ad un codice di condotta approvato di cui all'articolo 40 o ad un meccanismo di certificazione approvato di cui all'articolo 42 può essere Intesa quale elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo (art. 32)". Pertanto l'obiettivo è molto semplice: le aziende, per evitare il rischio di un enorme danno reputazionale, è bene adottino il codice di condotta che verrà presumibilmente stilato dalle associazioni di categoria e validato dal Garante della Privacy oppure affrontino un complesso meccanismo di certificazione (ad es. 27001 ISO/IEC).

Cosa prevedeva già il D. Lgs. 196/03	**Prescrizioni in materia di violazione dei dati personali (Data Breach), conseguenti al recepimento in Italia della direttiva europea 2009/136/CE.** Il recepimento è avvenuto tramite il D. Lgs. 69/12 che ha modificato in modo significativo il D. Lgs. 196/03 relativamente al trattamento dei dati personali e alla tutela della vita private. L'Autorità Garante per la protezione dei dati personali ha adottato, di conseguenza, il "Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach)" prevedendo: + la riaffermazione dell'esigenza di implementare una "Politica per la sicurezza"; + il rafforzamento dell'importanza dell'analisi dei rischi anche per individuare adeguate misure ex ante ed ex post rispetto alla violazione dei dati personali;

- l’adozione di misure per l’intelligibillità dei dati (essenziali per minimizzare anche il rischio di effettuare comunicazioni ai contraenti/altre persone);
- l’attuazione di misure atte a rendere i dati trattati indisponibili al termine delle attività svolte su di essi;
- l’adozione di misure specifiche volte a mitigare il rischio connesso alla portabilità dei dispostivi portatili;
- l’istituzione di obblighi di comunicazione da Fornitore a Garante;
- l’’istituzione di obblighi, in determinati casi, di comunicazione da Fornitore ai Contraenti/altre persone;
- l’’istituzione di obblighi di comunicazione da Affidatario a Fornitore;
- l’inventario delle Data Breaches che assume importanza strategica anche ai fini del sistema sanzionatorio.

DATA BREACH E SERVIZI CLOUD



In sintesi:

1. Se i controlli di sicurezza e il loro ambito sono negoziati nel contratto, la responsabilità è chiaramente “spostata” maggiormente sul fornitore del servizio Cloud: livelli di servizio, privacy e compliance sono tutte questioni inserite nei contratti;
2. la protezione della piattaforma rientra tra le responsabilità del provider, ma assicurare le applicazioni sviluppate sulla piattaforma e la loro sicurezza è un'attività che si riferisce al cliente: responsabilità ripartita tra fornitore e cliente;
3. la responsabilità di proteggere i dati appartiene al provider, le attività connesse al cliente: responsabilità maggiore del cliente.

8.La base giuridica

Rif.	Descrizione
Consenso	Il consenso dell'interessato autorizza il trattamento dei dati. Il consenso deve essere specifico, cioè legato ad una finalità precisa. Se il trattamento è basato sul consenso, il Titolare del trattamento deve fornire l'informativa e garantire la portabilità dei dati. In realtà, le autorità di protezione incoraggiano attivamente le imprese a superare l'intero processo di acquisizione del consenso per il trattamento dei dati personali. Questo perché il "consenso" non è ritenuto affidabile, nel senso che poche persone in realtà prendono una decisione "specifica, informata ed inequivocabile". Ben pochi, infatti, leggono le informative in materia. Il consenso è ritenuto, quindi, un onere per le imprese difficile da attuare per come è configurato. Le persone non vogliono essere bombardate dagli odiosi cookie banner, e comunque un banner dovrebbe contenere molte più informazioni di quante generalmente ne contiene, degradando enormemente l'esperienza di navigazione online. Ecco perchè esistono molti casi nei quali la base giuridica del trattamento è diversa dal consenso. NON deve essere necessariamente documentato per iscritto, né è richiesta la forma scritta, anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i "dati sensibili").

Adempimento di obblighi contrattuali	Il trattamento è lecito se è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Sostanzialmente è una forma speciale di consenso. Occorre, ovviamente l'informativa, e deve essere garantita la portabilità dei dati.
Obblighi di legge	Nel caso di trattamento dei dati necessario per l'adempimento di obblighi derivanti da Legge, Regolamento o Normativa Comunitaria, non occorre consenso, non si deve garantire la portabilità dei dati, ma è necessario fornire l'informativa, nella quale deve essere indicata la base giuridica del trattamento. In questo caso, la finalità deve essere specificata per legge.
Interessi vitali della persona interessata o di terzi	Il trattamento è ammesso se è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Si può tuttavia utilizzare come base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione. In quest'ultimo caso non occorre consenso, non si deve garantire la portabilità dei dati, ma è indispensabile fornire l'informativa, nella quale deve essere indicata la base giuridica del trattamento. Si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si consideri art. 46).
Legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati	Il legittimo interesse prevalente ricorre quando il trattamento è necessario per il perseguimento dello stesso in riferimento al Titolare del trattamento o a terzi, alla condizione per la quale non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, con particolare riguardo ai minori. Non occorre consenso, non si deve garantire la portabilità dei dati, ma è necessario fornire

	l'informativa, nella quale deve essere indicata la base giuridica del trattamento. **Cosa cambia?** Il bilanciamento fra legittimo interesse del Titolare o del terzo e i diritti e le libertà dell'interessato NON SPETTA all'Autorità, ma è compito dello stesso Titolare; si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal nuovo pacchetto di protezione dati. Inoltre, il Regolamento chiarisce espressamente che l'interesse legittimo del Titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei ispettivi compiti.[1]
Interesse pubblico o esercizio di pubblici poteri	Il 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 (tramite Legge statale o dell'Unione) non richiede consenso, né si deve garantire la portabilità dei dati, ma occorre fornire l'informativa nella quale deve essere indicata la base giuridica del trattamento. La finalità deve essere specificata per Legge.

[1] Il Regolamento offre alcuni criteri per il bilanciamento in questione (si consideri art. 47) e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto (*WP217*).

Si confermano, inoltre, nella sostanza, i **requisiti indicati dall'Autorità nei propri provvedimenti in materia di bilanciamento di interessi** [si veda, per esempio, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992 con riguardo ad alcune tipologie di trattamento di dati biometrici; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 con riguardo all'utilizzo della videosorveglianza; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6068256 in merito all'utilizzo di sistemi di rilevazione informatica anti-frode; ecc.] con particolare riferimento agli esiti delle verifiche preliminari condotte dall'Autorità, con eccezione, ovviamente, delle disposizioni che il Regolamento ha espressamente abrogato (per es.: obbligo di notifica dei trattamenti). I Titolari sono di per sè chiamati a condurre la propria valutazione alla luce di tutti questi principi.

9. DPO (o RDP)

Sono qui riportati gli elementi principali di cui alla guida del gruppo di lavoro “Articolo 29”: http://194.242.234.211/documents/10160/0/WP+243+-+Linee-guida+sui+responsabili+della+protezione+dei+dati+%28RPD%29.pdf

In base all’art. 37, paragrafo 1, del G.D.P.R., la nomina di un RPD è obbligatoria in tre casi specifici[2]:

1) **se il trattamento è svolto da un’Autorità o da un Organismo pubblici;**
2) **se le attività principali del Titolare o del Responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;**
3) **se le attività principali del Titolare o del Responsabile consistono nel trattamento su larga scala di categorie particolari di dati[3] o di dati personali relativi a condanne penali e reati.**

Il Gruppo di lavoro “Articolo 29” fornisce indicazioni sui criteri e sulle formulazioni utilizzati all’art. 37, paragrafo 1.

2 Si osservi che, in base all’art. paragrafo 4, il diritto dell’Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.

3 Ai sensi dell’articolo 9, si tratta dei dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l’appartenenza sindacale, oltre al trattamento di dati genetici e biometrici al fine dell’identificazione univoca di una persona fisica e di dati relativi alla salute, alla vita o agli orientamenti sessuali di una persona fisica.

"AUTORITÀ PUBBLICA O ORGANISMO PUBBLICO"

Nel Regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo di lavoro ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico. In questi casi, la nomina di un RPD è obbligatoria.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri[4] non pertengono esclusivamente alle autorità e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

A) ATTIVITÀ PRINCIPALI

L'art. 37, paragrafo 1, lettere b) e c), del G.D.P.R. contiene un riferimento alle "attività principali del Titolare del trattamento o del Responsabile del trattamento". Nel considerando 97 si afferma che le attività principali di un Titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal Titolare del trattamento o dal Responsabile del trattamento.

[4] Articolo 6, paragrafo 1, lettera e).

B) LARGA SCALA

In base all'art. 37, paragrafo 1, lettere b) e c), del G.D.P.R. occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel Regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito ricomprendendo, in particolare, "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*".

In realtà, è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; Il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

1) **il numero di soggetti interessati dal trattamento, in termini assoluti, ovvero espressi in percentuale della popolazione di riferimento**;
2) **il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento**;
3) **la durata, ovvero la persistenza, dell'attività di trattamento**;
4) **la portata geografica dell'attività di trattamento**.

C) MONITORAGGIO REGOLARE E SISTEMATICO

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del G.D.P.R.; tuttavia, il considerando art. 24 menziona il "*monitoraggio del comportamento di detti interessati*" ricomprendendovi tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

1) che avviene in modo continuo, ovvero a intervalli definiti per un arco di tempo definito;
2) ricorrente o ripetuto a intervalli costanti;
3) che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

1) che avviene per sistema;
2) predeterminato, organizzato o metodico;
3) che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
4) svolto nell'ambito di una strategia.

D) CATEGORIE PARTICOLARI DI DATI

Le disposizioni dell'art. 37, paragrafo 1, lettera c), riguardano il trattamento di categorie particolari di dati ai sensi dell'art. 9 e di dati personali relativi a condanne penali e a reati di cui all'art. 10. Nonostante l'utilizzo della congiunzione "e" nel testo inglese ("and"), non vi sono motivazioni sistematiche che impongano l'applicazione simultanea dei due criteri. Pertanto, il testo deve essere interpretato come se recasse la congiunzione "o". [NB: il testo italiano del regolamento reca già la congiunzione "o"].

10. TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

Il Regolamento:

+ disciplina la contitolarità del trattamento (art. 26) e impone ai Titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli Interessati i quali hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

+ fissa più dettagliatamente *(rispetto all'art. 29 del Codice)* le **caratteristiche dell'atto con cui il Titolare designa un Responsabile del Trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il Responsabile fornisca "garanzie sufficienti" – quali, in particolare, la natura, la durata e le finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal Titolare e, in via generale, delle disposizioni contenute nel regolamento;

+ consente la **nomina di Sub-Responsabili del trattamento** da parte di un responsabile *(si veda art. 28, paragrafo 4)* per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano Titolare e Responsabile primario; quest'ultimo **risponde dinanzi al Titolare dell'inadempimento dell'eventuale Sub-Responsabile,** anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" *(si veda art. 82, paragrafo 1 e paragrafo 3)*;

+ prevede **obblighi specifici in capo ai Responsabili del Trattamento**, in quanto distinti da quelli pertinenti ai rispettivi Titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti**

svolti *(ex art. 30, paragrafo 2)*; l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti *(ex art. 32 regolamento)*; la **designazione di un RPD-DPO** (si vedano anche le linee-guida in materia di responsabili della protezione dei dati recentemente pubblicate dal Gruppo "Articolo 29" dopo essere state sottoposte a consultazione pubblica, disponibili qui anche nella versione in italiano: **www.garanteprivacy.it/rpd**), nei casi previsti dal Regolamento o dal diritto nazionale *(si veda art. 37 del regolamento)*. Si ricorda, inoltre, che **anche il Responsabile** non stabilito nell'Ue dovrà **designare un Rappresentante** in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del Regolamento – diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice;

+ definisce **caratteristiche soggettive e responsabilità di Titolare e Responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la **figura dell'"Incaricato" del Trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile" *(si vedano, in particolare, artt. 4, n. 10, del Regolamento)*.

RACCOMANDAZIONI

I Titolari di Trattamento debbono valutare attentamente l'esistenza di eventuali situazioni di contitolarità (si vedano, in proposito, le indicazioni fornite dal Garante in vari provvedimenti, fra cui **http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785**, essendo obbligati in tal caso a stipulare l'accordo interno di cui parla l'art. 26, paragrafo 1, del Regolamento. Sarà necessario, in particolare, individuare il "punto di contatto per gli Interessati" previsto dal suddetto articolo ai fini dell'esercizio dei diritti previsti dal Regolamento.

I Titolari di Trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del Regolamento. Dovranno essere apportate le necessarie integrazioni o modifiche entro il 25 maggio 2018, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti. La Commissione e le autorità nazionali di controllo (fra cui il Garante) stanno valutando la definizione di clausole contrattuali modello da utilizzare a questo scopo.

Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del Regolamento, in particolare alla luce del principio di "responsabilizzazione" di Titolari e Responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del Regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che Titolari e i Responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli Incaricati di Trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante (si veda art. 30 del Codice e, fra molti, **http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1507921**, ovvero **http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1508059** per quanto riguarda la pubblica amministrazione, ovvero **http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953** in materia di tracciamento delle attività bancarie) in quanto

misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento *(si veda art. 24, paragrafo 1, del regolamento)*.

PROBLEMATICHE RELATIVE AL RESPONSABILE INTERNO

Se per la figura dell'Incaricato non sembrano esserci particolari problematiche, la questione appare differente per la figura del **Responsabile interno** dove è maggiormente diffusa una concezione non sempre coerente.

In primo luogo, bisogna avere ben presente che con il G.D.P.R. non può più bastare la limitata visione a livello nazionale delle questioni sulla Data Protection. Dal 25 maggio 2018, infatti, con l'abrogazione della Direttiva 45/196 /CE, non sarà più in essere il mutuo riconoscimento che valeva per le singole leggi nazionali attuative della Direttiva madre. Inoltre, gli Interessati residenti in altri Stati membri della UE potranno rivolgersi alle DPA del proprio Paese qualora ritengano che i propri dati personali siano stati oggetto di un trattamento non legittimo da parte di un'azienda italiana. La distinzione tra Responsabile interno e Responsabile esterno è una prassi operativa italiana che non trova riscontri normativi nella direttiva 95/46/CE, nel Codice Privacy D.lgs 196/2003 e tanto meno nel Regolamento (UE) 2016/679 dalla cui analisi appare piuttosto evidente che la figura del Responsabile interno risulta per diversi aspetti non più compatibile con il nuovo dettato normativo.

Secondo il Regolamento, il **Responsabile del Trattamento** (Art.4.8) è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che **tratta dati personali per conto del titolare del trattamento**".

Appare evidente dagli articoli 4.10 e 29 che le rispettive espressioni "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile" e "chiunque agisca sotto la autorità del Responsabile del Trattamento o sotto quella del Titolare del trattamento" si riferiscono sostanzialmente a categorie di soggetti con ruoli subalterni interni, come dipendenti e collaboratori; ruoli riconducibili alla figura dell'ex incaricato del Codice Privacy. Dall'articolo 29 del G.D.P.R. appare inoltre evidente emergere la netta distinzione tra il personale dipendente e le figure che invece hanno il potere di definire finalità e mezzi del trattamento (Titolari) o di trattare i dati per conto del titolare del trattamento (Responsabili).

Vi sono inoltre una serie di obblighi e disposizioni contrattuali che il G.D.P.R. pone in seno ai Responsabili del trattamento, **che risultano non compatibili con una figura interna**, come molte delle disposizioni previste all'articolo 28.3, che appaiono applicabili solo a un responsabile esterno.

Va inoltre considerata l'esposizione al rischio della responsabilità solidale:

- è risarcibile qualsiasi danno causato da una violazione del regolamento (Art. 82.1);
- il Titolare del Trattamento è responsabile e risponde per il danno cagionato dal suo trattamento (Art. 82.2);
- i Responsabili del trattamento sono responsabili in solido per il risarcimento del danno con titolari, contitolari e altri responsabili Art. 26.3, Art.28, Art. 82.4.

Alla luce di tutto questo, non sembra più praticabile la nomina indiscriminata di Responsabili interni del trattamento, solo perché ricoprono la qualifica aziendale di capi reparto o di dirigenti di unità operativa, quando nelle loro effettive mansioni privacy è prevista la sola esecuzione di poche istruzioni operative. In questo caso si propone, quindi, di inserire queste figure all'interno di un ben strutturato organigramma privacy dell'azienda, dove verranno specificati e dettagliati ruoli, compiti e mansioni dei vari dipendenti, ciascuno dei quali dovrà ricevere dal Titolare istruzioni e formazione complete e adeguate al ruolo loro assegnato.

11. CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Rif.	Consenso Regolamento UE 679/2016
Art. 4	Il **consenso,** in base al nuovo Regolamento Generale (art. 4 G.D.P.R.), è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano sono oggetto di trattamento. Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo. Il consenso è **una delle basi giuridiche del trattamento,** nell'ambito del regolamento generale per la protezione dei dati personali.
Caratteristiche	Il consenso deve essere, quindi: + **inequivocabile;** + **libero;** + **specifico;** + **informato;** + **verificabile;** + **revocabile.** Consenso **inequivocabile** vuol dire che non è necessario che sia esplicito, ma può anche essere implicito (non tacito), purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'Interessato abbia voluto

comunicare il consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche i form precompilati e caselle già prespuntate). Il consenso deve, invece, essere esplicito (art. 9 G.D.P.R.) nel caso di trattamento di dati sensibili o nel caso di processi decisionali automatizzati (es. profilazione).

Il consenso deve essere dato **liberamente**, il ché significa che l'Interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso. L'art. 7 del G.D.P.R. chiarisce che "*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*".

Ad esempio, nel caso di pubblicità commerciale, **il consenso deve essere separato rispetto al consenso per la prestazione contrattuale richiesta dall'utente**, perchè l'utente deve avere la possibilità di addivenire al contratto senza dover subire il ricatto di ricevere pubblicità commerciale.

Il consenso deve essere **specifico**, cioè relativo alla finalità per la quale è eseguito quel trattamento. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità (Considerando art. 32 G.D.P.R.). Quindi, i dati dovranno essere pertinenti al consenso fornito e, in caso di modifiche del trattamento, occorre richiedere un nuovo consenso. Per cui avremo un consenso per il marketing diretto, un consenso per la profilazione, ecc...

Il consenso deve essere **informato**, occorre cioè che l'interessato sia posto nella condizione di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge.

Consenso **verificabile** non vuol dire che il consenso debba essere documentato per iscritto, né che ne sia richiesta la forma scritta (anche se in alcune ipotesi, riferite ai dati sensibili, per esempio), può essere preferibile perché consente più facilmente di provarlo, facilitando quindi le verifiche da parte dell'autorità), ma che l'azienda deve essere in grado di dimostrare che l'interessato lo ha conferito con riferimento a quello specifico trattamento (quindi distinguendo tra i vari trattamenti).

Il consenso **deve essere revocabile** in qualsiasi momento. La revoca deve essere facile, al pari di concederlo. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento), a meno che non sussista una differente base giuridica per continuare il trattamento.

Infine, **il consenso non può costituire la base giuridica** del trattamento in caso di evidente squilibrio tra le parti. In tal caso sarebbe preferibile trattare i dati su base giuridica differente.

Non esiste più una specifica definizione di dati personali "sensibili" o di dati personali "giudiziari". Tuttavia, l'art. 9 individua in generale le "**categorie particolari di dati personali**" nelle informazioni "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una*

Dati "sensibili"

persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica"; mentre il successivo articolo 10 del Regolamento disciplina il trattamento dei *"dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza*".

Il Regolamento introduce comunque una nuova definizione limitata ai "***dati relativi alla salute***" intesi quali 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*».

Il trattamento dei dati (ex) sensibili è addirittura vietato come regola generale, derogabile nei casi specifici elencati dall'art.9. Gli Stati membri possono comunque mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Per quanto riguarda il trattamento dei dati personali relativi alle **condanne penali e ai reati o a connesse misure di sicurezza**, vale il principio, già noto al Codice della Privacy, per il quale il trattamento dei dati giudiziari deve avvenire soltanto sotto il controllo dell'autorità pubblica o, se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri, prevedere garanzie appropriate per i diritti e le libertà degli interessati. Il consenso costituisce **l'unica base giuridica utile per il trattamento di questi dati**. A parte il trattamento per l'attività giornalistica, che è a forma libera per qualsiasi tipo di dato. **Deve essere esplicito**.

12. TRASFERIMENTI DI DATI VERSO PAESI TERZI E ORGANISMI INTERNAZIONALI

In primo luogo, **viene meno il requisito dell'autorizzazione nazionale** *(si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2)*. Ciò significa che il trasferimento dei dati verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione – ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del Regolamento – potrà avere inizio senza attendere l'autorizzazione nazionale del Garante, a differenza di quanto precedentemente previsto dal Codice.

Tuttavia, **l'autorizzazione del Garante sarà ancora necessaria** qualora un Titolare desideri utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi** stipulati tra autorità pubbliche.

Il Regolamento consente di ricorrere anche a **codici di condotta, ovvero a schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'art. 46. Ciò significa che i **Titolari o i Responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta** o allo schema di certificazione, ove questi disciplinino anche, o esclusivamente, i trasferimenti di dati verso Paesi terzi, al fine di legittimarli. **Tuttavia** *(si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2)*, tali Titolari dovranno **assumere**, inoltre, **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati.

Il Regolamento vieta trasferimenti di dati verso Titolari o Responsabili in un Paese terzo sulla base di **decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo**, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati *(si veda art. 48)*. Si potranno utilizzare, tuttavia, gli altri presupposti e, in particolare, le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve ricordare che il Regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un **interesse pubblico riconosciuto dal diritto dello Stato membro** del Titolare o dal diritto dell'Ue *(si veda art. 49, paragrafo 4)* – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

Il regolamento **fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme**. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del Regolamento – ossia, **è previsto, in ogni caso, l'intervento del Comitato europeo per la protezione dei dati** *(si veda art. 65, paragrafo 1, lettera d))*.

Il Regolamento *(si veda Capo V)* **ha confermato l'approccio attualmente 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:

i) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea *(si veda art. 44, comma 1, lettera b), del Codice)*;

ii) 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) *(si veda Art. 44, comma 1, lettera a) del Codice)*.

iii) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni *(corrispondenti in parte alle disposizioni dell'art. 43, comma 1, del Codice)*.

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 *(si vedano art. 45, paragrafo 9, e art. 96)*. 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#1). Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi *(si veda art. 46, paragrafo 5)*, sino a loro eventuale modifica.

13. DIRITTI DEGLI INTERESSATI

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 nei casi di particolare complessità; il termine di un mese è stabilito anche in caso di diniego.

Spetta al Titolare valutare la complessità del riscontro all'Interessato e **stabilire l'ammontare dell'eventuale contributo** da sottoporgli nel caso di **richieste manifestamente infondate o eccessive** (anche ripetitive) *(art. 12.5); questo anche a* differenza di quanto prevedono gli artt. 9, comma 5, e 10, commi 7 e 8, del Codice, laddove si fa riferimento a **"più copie" dei dati personali** nel caso del diritto di accesso *(art. 15, paragrafo 3)*; in quest'ultimo caso, il Titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'Interessato** deve avvenire, di regola, in **forma scritta**, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere fornito **oralmente solo se così richiede l'Interessato** stesso *(art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3)*.

Modalità per l'esercizio dei diritti

La risposta fornita all'Interessato non deve essere solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile** e prevedere l'utilizzo di un **linguaggio semplice e chiaro**.

Il Titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'Interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Benché sia il solo Titolare a dover dare riscontro** in caso di esercizio dei diritti *(artt. 15-22)*, il

Responsabile è tenuto a collaborare con lo stesso ai fini dell'esercizio dei diritti degli Interessati *(art. 28, paragrafo 3, lettera e)*.

L'esercizio dei diritti è, in linea di principio, gratuito per l'Interessato, ma possono esservi eccezioni *(si veda il paragrafo "Cosa cambia")*. Il Titolare ha il diritto di chiedere informazioni necessarie ad identificare l'Interessato, e quest'ultimo, ha il dovere di fornirle, secondo modalità idonee *(si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6)*.

Sono ammesse **deroghe ai diritti** riconosciuti dal Regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23, nonché di altri articoli relativi ad ambiti specifici *(si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).*
In questo senso, in via generale, possono continuare ad essere applicate **tutte le deroghe previste dall'art. 8, comma 2, del Codice in quanto compatibili** con le disposizioni citate. Al riguardo, il Garante sta valutando la piena rispondenza delle disposizioni citate in tale articolo del Codice con i requisiti fissati per la legislazione nazionale dall'articolo 23, paragrafo 2, del Regolamento.

Diritto di accesso (art. 15)

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

	Fra le informazioni che il Titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.
Diritto di cancellazione (diritto all'oblio) (art.17)	Si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato pubblicandoli, ad esempio, su un sito web) di informare della richiesta di cancellazione altri Titolari che trattano i medesimi dati, sotto qualsiasi forma, compresi link, copie o riproduzioni (si veda art. 17, paragrafo 2). Il diritto in parola ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del D. Lgs. 196/03, poiché lIinteressato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).
Diritto di limitazione del trattamento (art. 18)	Si tratta di un diritto **diverso e più esteso rispetto al "blocco" del** trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'Interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del Titolare) o si opponga al loro trattamento ai sensi dell'art. 21 del Regolamento (in attesa della valutazione da parte del Titolare). Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato, a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Diritto alla portabilità dei dati (art. 20)	Si tratta di uno dei nuovi diritti previsti dal Regolamento, anche se non del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico). **Non si applica ai trattamenti non automatizzati** (quindi non si applica agli archivi o registri cartacei) e sono altresì previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'Interessato o sulla base di un contratto stipulato con lo stesso** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al Titolare *(si veda il considerando 68 per maggiori dettagli)*. Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'Interessato, se tecnicamente possibile.