La nuova disciplina della privacy prevista dal regolamento UE 679/2016

1 premessa

Con il regolamento UE 27.4.2016 n. 679 sono state introdotte alcune novità in materia di *priva*

Tale regolamento, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, è entrato in vigore il 24.5.2016, ma sarà applicabile dal prossimo 25.5.2018.

Mancano ancora le norme di coordinamento rispetto alla disciplina prevista dal vigente Codice della *privacy* (di cui al DLgs. 196/2003), che, quindi, alla data del 25.5.2018, rimarrà in vigore, ma compatibilmente con il nuovo regolamento.

Alla data della presente circolare, risulta l'approvazione da parte del Consiglio dei Ministri, in esame preliminare, solo di uno schema di DLgs. recante le disposizioni per l'adeguamento della normativa nazionale al nuovo reg. UE 679/2016, in attuazione dell'art. 13 della L. 25.10.2017 n. 163 (legge di delegazione europea 2016-2017). Il suddetto DLgs., una volta emanato, sostituirà il vigente Codice della *privacy* e costituirà, insieme al regolamento europeo, la nuova disciplina in materia di *privacy*.

Si segnala, ad oggi, l'emanazione del DPR 15.1.2018 n. 15, recante il "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia*", che in premessa richiama il regolamento europeo.

Nell'ambito delle attività preparatorie all'adeguamento *privacy*, sono intervenuti il Garante per la protezione dei dati personali e il Gruppo di lavoro *ex* Articolo 29 della direttiva CE 95/46 con la pubblicazione di alcuni documenti interpretativi e schede informative.

1.1 Oggetto e finalità del regolamento

Le disposizioni contenute nel reg. UE 679/2016 (art. 1 par. 1) riguardano la protezione delle persone fisiche (così come per il Codice della *privacy*, che esclude il trattamento dei dati relativi a persone giuridiche) con riferimento:

- al trattamento dei dati personali;
- alla libera circolazione di tali dati.

1.2 Ambito di applicazione materiale

Il reg. UE 679/2016 (art. 2) trova applicazione con riferimento ai seguenti trattamenti:

- trattamento automatizzato, in maniera parziale o totale, di dati personali;
- trattamento non automatizzato di dati personali contenuti in un archivio o destinati ad essere ivi inclusi.

Sono esclusi, in particolare, i trattamenti di dati personali effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

In considerazione del fatto, poi, che per "dato personale" si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*" (art. 4 n. 1), sono esclusi dall'applicazione del regolamento anche i dati trattati in forma anonima e che non consentono l'identificazione del soggetto interessato.

1.3 Ambito di applicazione territoriale

Il reg. UE 679/2016 (art. 3) si estende al trattamento dei dati personali effettuato:

- nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento avvenga nell'Unione europea o meno;
- da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, per dati di interessati che si trovano nell'Unione, quando le attività di trattamento riguardano:
- l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
- il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione;
- da un titolare del trattamento non stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

2 Figure professionali

Nell'ambito dei soggetti coinvolti nel trattamento dei dati personali, il reg. UE 679/2016 (Capo IV, artt. 24 – 43) continua a prevedere, rispetto al Codice della *privacy* (artt. 28 – 29), le figure del titolare del trattamento dei dati e del responsabile del trattamento dei dati.

Il regolamento, poi, disciplina la nuova figura del responsabile per la

protezione dei dati personali.

2.1 Titolare, responsabile e incaricato del trattamento dei dati

Il reg. UE 679/2016 definisce in maniera più precisa ruoli e compiti del titolare e del responsabile del trattamento dei dati. Tali qualifiche possono essere assunte da una persona fisica o giuridica, un'autorità pubblica, un servizio o altro organismo (art. 4 n. 7 e 8).

Non sembra essere esclusa, poi, la presenza dell'incaricato del trattamento, anche se non espressamente prevista come nel vigente Codice della *privacy* (art. 30), nell'ambito delle "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*" (art. 4 n. 10).

Titolare del trattamento

Il titolare del trattamento è il soggetto che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (artt. 24, 26 e 27 del reg. UE 679/2016).

Rispetto al Codice della *privacy*, viene codificata l'ipotesi della contitolarità del trattamento, identificata come compresenza di due o più titolari del trattamento che determinano "*congiuntamente*" finalità e mezzi del trattamento, con definizione mediante accordo delle rispettive responsabilità e compiti, oltre che dei rispettivi ruoli e rapporti con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato, il quale, indipendentemente da tale accordo, può esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

In caso di trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato, però, da un titolare del trattamento (o da un responsabile del trattamento) che non è stabilito nell'Unione, il titolare del trattamento (o il responsabile del trattamento) deve designare, salvo alcune eccezioni, per iscritto un rappresentante nell'Unione.

Responsabile del trattamento

Il responsabile del trattamento è il soggetto che tratta dati personali per conto del titolare del trattamento (art. 28 del reg. UE 679/2016).

Rispetto al Codice della *privacy*:

- viene prevista una più specifica definizione dei rapporti fra titolare e responsabile, che deve avvenire mediante il ricorso a un contratto (o altro atto giuridico), in forma scritta (anche in formato elettronico), con uno specifico contenuto;
- il responsabile del trattamento può ricorrere ad un altro responsabile solo su autorizzazione scritta (specifica o generale) del titolare del trattamento;
- può essere nominato un sub-responsabile del trattamento, per specifiche attività di trattamento, nel qual caso occorre definire i rapporti mediante un contratto o altro atto giuridico.

La violazione del regolamento da parte del responsabile del trattamento, determinando finalità e mezzi del trattamento stesso, comporta l’assunzione diretta della qualifica di titolare del trattamento.

Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate onde assicurare la conformità del trattamento al regolamento e alla tutela dei diritti dell’interessato (dimostrata anche mediante il ricorso a Codici di condotta o meccanismi di certificazione).

Contenuto del contratto

Aspetti generali

Il contratto deve prevedere:

- la materia disciplinata;
- la durata del trattamento;
- la natura e finalità del trattamento;
- il tipo di dati personali;
- le categorie di interessati;
- gli obblighi e diritti del titolare del trattamento.

Aspetti specifici	Il contratto deve prevedere che il responsabile del trattamento: · proceda al trattamento dei dati solo su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo sussista un obbligo giuridico stabilito dal diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento e di cui deve essere informato prima del trattamento il titolare (salvo divieto per rilevanti motivi di interesse pubblico); · garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; · adotti tutte le misure di sicurezza; · rispetti le condizioni stabilite per la nomina di un altro responsabile del trattamento; · assista il titolare, tenuto conto della natura del trattamento, con misure tecniche e organizzative adeguate per l'adempimento da parte del titolare alle richieste dell'interessato per l'esercizio dei suoi diritti; · assista il titolare, tenuto conto della natura del trattamento e delle informazioni a disposizione, nel garantire il rispetto degli obblighi per la sicurezza dei dati personali e per la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva; · su scelta del titolare del trattamento, cancelli o restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento, e cancelli le copie esistenti, salvo sia prevista dal diritto dell'Unione o degli Stati membri la conservazione dei dati; · metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto dei sopra esposti obblighi, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

2.2 Responsabile della protezione dei dati

Il reg. UE 679/2016 (artt. 37 – 39) introduce la nuova figura professionale del responsabile della protezione dei dati – RPD (o *Data Protection Officer* – DPO), di cui si forniscono le principali caratteristiche nella seguente tabella.

Nomina	La nomina dell'RPD è obbligatoria per: · l'autorità pubblica o l'organismo pubblico (salvo il trattamento dei dati sia effettuato dalle autorità giurisdizionali nell'esercizio delle funzioni giurisdizionali); · tutti i soggetti la cui attività principale consista in trattamenti che, per la loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; · tutti i soggetti la cui attività principale consista nel trattamento, su larga scala, di categorie particolari di dati personali (nell'ambito dei quali sono compresi i dati definiti dal Codice della *privacy* come "sensibili", oltre ai nuovi dati genetici e biometrici) e i dati relativi a condanne penali e reati (artt. 9 e 10 del reg. UE 679/2016).
Qualifica e designazione	L'RPD viene designato dal titolare del trattamento e dal responsabile del trattamento: · in funzione delle qualità professionali (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati) e della capacità di assolvere i propri compiti; non sono necessarie attestazioni formali o titoli professionali specifici; · ricorrendo a un proprio dipendente (RPD interno) o a un soggetto esterno (RPD esterno), in quest'ultimo caso mediante il ricorso ad un contratto di servizi. È possibile per un gruppo di imprese o di soggetti pubblici nominare un unico RPD.
Compiti	L'RPD deve svolgere i seguenti compiti minimi: · informare e fornire consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti, in merito agli obblighi derivanti dal regolamento; · verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi *auditors*; · fornire, se richiesto, pareri in merito alla valutazione di impatto sulla protezione dei dati e sorvegliare i relativi adempimenti; · fungere da punto di contatto con l'autorità di controllo o, eventualmente, consultarla di propria iniziativa. Nell'esecuzione di tali compiti, l'RPD: · deve essere "*sostenuto*", mediante il rilascio delle risorse necessarie; · non deve ricevere alcuna istruzione; · non è rimosso o penalizzato.
Obblighi	È tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti (che possono essere anche altri, purché non integrino un conflitto di interessi).

Adempimenti	I dati di contatto del responsabile della protezione dei dati devono essere pubblicati e comunicati all'autorità di controllo da parte del titolare del trattamento e dal responsabile del trattamento.

3 Adempimenti del titolare del trattamento e del responsabile del trattamento

In capo al titolare del trattamento e al responsabile del trattamento sono stati:

- dettagliati e/o modificati alcuni adempimenti già previsti dal Codice della *privacy*, ad esempio in materia di modalità di trattamento dei dati, di acquisizione del consenso e di rilascio dell'informativa;
- introdotti nuovi compiti, fra i quali tenere un registro delle attività di trattamento ed effettuare una valutazione di impatto sulla protezione dei dati.

3.1 Modalità di trattamenti dEi dati

Il titolare del trattamento deve previamente istruire tutti coloro che siano autorizzati ad accedere e trattare i dati personali, compreso il responsabile del trattamento (art. 29 del reg. UE 679/2016).

Costituiscono principi generali del trattamento (art. 5 del reg. UE 679/2016):

- la liceità, la correttezza e la trasparenza nei confronti dell'interessato;
- la limitazione delle finalità (determinate, esplicite e legittime);
- la minimizzazione dei dati, che devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- l'esattezza, con aggiornamento dei dati se necessario;
- la limitazione della conservazione;
- l'integrità e la riservatezza;
- la responsabilizzazione del titolare del trattamento, il quale è competente per il rispetto dei principi sopra esposti e sul quale grava l'onore di prova.

Con specifico riguardo alla liceità del trattamento, il regolamento conferma che questo deve trovare fondamento su un'idonea base giuridica, che corrisponde in linea di massima a quella del vigente Codice della *privacy* (artt. 11 e 23).

Il trattamento è lecito se ricorrono i seguenti presupposti (art. 6 del reg. UE 679/2016):

- consenso dell'interessato per una o più specifiche finalità;
- adempimento di obblighi contrattuali, di cui l'interessato è parte o di misure precontrattuali;
- obblighi di legge cui è soggetto il titolare del trattamento;
- interessi vitali della persona interessata o di terzi;
- interesse pubblico o esercizio di pubblici poteri;

- interesse legittimo del titolare del trattamento o di terzi cui i dati vengono comunicati, la cui prevalenza – rispetto al Codice della *privacy* – è valutata dallo stesso titolare del trattamento (per effetto del principio di responsabilizzazione).

3.2 Acquisizione del consenso

Come già previsto dal Codice della *privacy* (art. 23), il consenso deve essere libero, specifico rispetto alle finalità del trattamento (o per finalità compatibili), informato.

Rispetto però al Codice della *privacy*, che stabilisce espressamente la forma scritta per la prova del consenso al trattamento dei dati in generale e per la stessa validità in caso di dati sensibili, il regolamento non precisa le modalità di espressione del consenso.

Il regolamento richiede il consenso "*esplicito*" solo per:

- categorie particolari di dati;
- le decisioni basate su trattamenti automatizzati (compresa la profilazione).

La richiesta di consenso, qualora inserita all'interno di una dichiarazione scritta, deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato e deve essere resa in forma comprensibile e facilmente accessibile, con linguaggio semplice e chiaro.

Il consenso dei minori è valido a partire dai 16 anni, mentre prima occorre il consenso dei genitori o di chi ne fa le veci.

Categorie particolari di dati personali

Sono inclusi nella nuova definizione di "categorie particolari di dati" quelli attualmente previsti dal Codice della *privacy* come dati "sensibili", quindi i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oltre ai dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del reg. UE 679/2016 e art. 4 co. 1 lett. d) del Codice della *privacy*).

In tale categoria sono inclusi i nuovi riferimenti ai dati genetici e dati biometrici intesi a identificare in modo univoco una persona fisica.

Per il trattamento dei suddetti dati è, in generale, prescritto il divieto generale di trattamento. Costituiscono eccezione, oltre al consenso, fra l'altro, l'esecuzione di un contratto di lavoro e le connesse esigenze di sicurezza/protezione sociale, nonché la difesa di un diritto in sede giudiziaria.

Dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi a condanne penali e reati – sostanzialmente corrispondenti a quelli oggi definiti

“giudiziari” – deve avvenire, in maniera alternativa, sotto il controllo della autorità pubblica o previa autorizzazione proveniente da norme dell’Unione e del singolo Stato membro, che prevedano garanzie appropriate per i diritti e le libertà degli interessati (art. 10 del reg. UE 679/2016 e art. 4 co. 1 lett. e) del Codice della *privacy*).

Processi decisionali automatizzati

Il reg. UE 679/2016 (art. 22) codifica espressamente, rispetto al Codice della *privacy*, il diritto dell’interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato dei dati che produca effetti giuridici che lo riguardano o che comunque incida significativamente sulla sua persona.

In tale ambito, viene ricompresa anche la profilazione, definita come “*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*” (art. 4 n. 4 del reg. UE 679/2016).

Il trattamento è vietato salvo l’acquisizione del consenso “*esplicito*” dell’interessato, o nei casi in cui tali operazioni siano necessarie per l’esecuzione di un contratto con l’interessato o sia autorizzata dal diritto dell’Unione o del singolo Stato membro.

Rimane comunque l’obbligo di apprestare garanzie adeguate ad assicurare il rispetto dei diritti dell’interessato, riguardanti la specifica informazione all’interessato, e del diritto di ottenere l’intervento umano, nonché di esprimere la propria opinione e di contestare la decisione.

È vietato l’utilizzo di categorie particolari di dati per scopi decisionali automatizzati, salvo che l’interessato abbia espresso il suo consenso esplicito o la decisione automatizzata sia necessaria per motivi di interesse pubblico. In entrambi i casi, devono sussistere misure tecniche e organizzative adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell’interessato.

Nell’informativa devono essere esplicitate le modalità e le finalità della profilazione. Inoltre, deve essere chiarita la logica inerente il trattamento e le conseguenze previste per l’interessato a seguito di tale tipo di trattamento (art. 13 del reg. UE 679/2016).

Trattamento dei dati nell’ambito dei rapporti di lavoro

Per quanto riguarda il trattamento dei dati nell’ambito dei rapporti di lavoro (art. 88), viene riconosciuta la possibilità per gli Stati membri di prevedere (con legge o tramite contratti collettivi) norme più specifiche “*per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell’ambito dei rapporti di*

lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro".

3.3 Informativa

Il reg. UE 679/2016 (artt. 13 e 14) riprende, rispetto al Codice della *privacy* (art. 13), l'obbligo di informativa, distinto sempre rispetto alla raccolta dei dati presso l'interessato o meno, prevedendo però un contenuto maggiormente dettagliato.

L'informativa deve:

- avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile e deve essere utilizzato un linguaggio chiaro e semplice;
- essere data per iscritto o con "*altri mezzi*" anche elettronici (ad esempio, nel caso di servizi *on line*), oralmente se richiesto dall'interessato (il Codice della *privacy* prevede solo in forma scritta od orale); è ammesso l'uso di icone.

Qualora i dati personali siano raccolti presso l'interessato, le informazioni devono essere fornite nel momento in cui i dati personali sono ottenuti.

Nel caso di dati personali non ottenuti presso l'interessato, le informazioni devono essere fornite:

- entro un termine ragionevole dall'ottenimento dei dati personali, comunque entro un mese, tenuto conto delle specifiche circostanze di trattamento dei dati;
- qualora i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato;
- qualora sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

Qualora le finalità cambino, occorre informarne l'interessato prima di procedere al trattamento ulteriore.

In entrambi i casi di informativa per dati raccolti presso l'interessato o meno, la stessa non va resa se e nella misura in cui l'interessato abbia già le informazioni.

Per la sola categoria della raccolta di dati non presso l'interessato, costituiscono casi di esclusione dell'informativa i seguenti:

- qualora la comunicazione risulti impossibile o implicherebbe uno sforzo sproporzionato (su valutazione del titolare del trattamento, invece che

del Garante per la protezione dei dati personali come previsto dal Codice della *privacy*);

- qualora l’ottenimento o la comunicazione siano 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;
- 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.

Contenuto dell'informativa

Informativa per il trattamento di dati raccolti presso l'interessato	Occorre rendere noto: · 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, se nominato; · le finalità del trattamento cui sono destinati i dati personali e la base giuridica del trattamento; · i legittimi interessi perseguiti dal titolare del trattamento o da terzi, qualora costituisca la base giuridica del trattamento; · gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; · 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 il riferimento alle garanzie appropriate od 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;
segue	· l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca, nei casi di trattamento basato sul consenso, anche di categorie particolari di dati; · il diritto di proporre reclamo a un'autorità di controllo; · se la comunicazione di dati personali è un obbligo legale o contrattuale o un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, oltre alle possibili conseguenze circa la mancata comunicazione di tali dati; · l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, in tali casi, le informazioni significative sulla logica utilizzata, oltre all'importanza e alle conseguenze previste di tale trattamento per l'interessato.

Contenuto dell'informativa	
Informativa per il trattamento di dati non ottenuti presso l'interessato	Occorre rendere noto le informazioni di cui sopra (con esclusione del riferimento alla comunicazione dei dati personali come obbligo legale o contrattuale), con l'aggiunta: · delle categorie di dati personali oggetto di trattamento; · della fonte da cui hanno origine i dati personali e, se del caso, dell'eventualità che i dati provengano da fonti accessibili al pubblico.

3.4 diritti degli interessati

Nell'ambito dei diritti previsti in capo all'interessato, vengono ripresi, rispetto al Codice della *privacy*, oltre all'informativa sul trattamento dei dati personali, i seguenti (artt. 12 – 23 del reg. UE 679/2016):

- diritto di accesso;
- diritto di rettifica;
- diritto di cancellazione (diritto all'oblio in forma rafforzata);
- diritto di opposizione.

Viene previsto, poi, il diritto alla limitazione al trattamento dei dati, che costituisce un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui al Codice della *privacy* (art. 7 co. 3 lett. b)).

Viene introdotto, infine, il nuovo diritto alla portabilità dei dati, che riguarda i trattamenti:

- basati sul consenso o su un contratto stipulato con l'interessato;
- effettuati con mezzi automatizzati.

Inoltre, si deve trattare di dati forniti direttamente dall'interessato al titolare del trattamento.

Modalità per l'esercizio dei diritti

Quanto alle modalità per l'esercizio dei diritti, rispetto al Codice della *privacy* (artt. 9 e 10):

- il termine per la risposta all'interessato è, per tutti i diritti, di un mese dal ricevimento della richiesta, estendibile fino a due mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato, anche in caso di diniego;
- il riscontro alle richieste presentate dagli interessati deve avvenire in forma scritta, anche elettronica; se la richiesta avviene con mezzi elettronici, nella medesima forma sono rese le informazioni (ove possibile e salva diversa indicazione dell'interessato);
- in generale le informazioni vanno rese in maniera gratuita; spetta al titolare, però, stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato qualora si tratti di richieste manifestamente infondate o eccessive, anche ripetitive, e, nell'ambito del diritto di accesso, nel caso di richiesta di più copie dei dati personali (tenuto

conto dei costi amministrativi sostenuti).

3.5 Principio di "*accountability*"

Viene introdotto il principio della c.d. "responsabilizzazione" (*accountability*) di titolari (e responsabili) del trattamento, che sono tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire e per dimostrare l'applicazione del regolamento, con gli aggiornamenti necessari (art. 24 del reg. UE 679/2016).

Pertanto, è il titolare che decide in maniera autonoma modalità, garanzie e limiti del trattamento dei dati personali, nel rispetto del regolamento e di alcuni criteri previsti (ad esempio, fra questi vi è il principio della *privacy* "*by design*" e "*by default*").

3.6 Principio della *privacy* "*by design*" e "*by default*"

Viene richiesto al titolare del trattamento di impostare da subito l'attività e la stessa organizzazione secondo i principi c.d. di "*privacy by design*" e "*privacy by default*", riducendo i trattamenti non necessari (art. 25 del reg. UE 679/2016).

In particolare:

- "*privacy by design*": occorre attuare adeguate misure tecniche e organizzative sin dall'atto della progettazione (quindi, prima di procedere al trattamento dei dati) e comunque al momento dell'esecuzione del trattamento; fra le misure vengono indicate espressamente la pseudonimizzazione e la minimizzazione;
- "*privacy by default*": i dati vengano trattati, per impostazione predefinita, esclusivamente per le finalità previste e per il periodo strettamente necessario (in maniera similare a quanto già previsto dal Codice della *privacy* con il principio di necessità); le misure devono garantire che i dati personali non siano resi accessibili a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

La conformità ai requisiti richiesti può essere dimostrata mediante il ricorso a meccanismi di certificazione.

3.7 Registro delle attività di trattamento

I titolari e i responsabili del trattamento devono tenere un registro delle operazioni di trattamento, in forma scritta, anche in formato elettronico (art. 30 del reg. UE 679/2016).

Sono escluse da tale obbligo le imprese o le organizzazioni con meno di 250 dipendenti, salvo che il trattamento:

- possa presentare un rischio per i diritti e le libertà dell'interessato;
- non sia occasionale;
- includa il trattamento di categorie particolari di dati o di dati personali relativi a condanne penali e a reati.

Contenuto del registro	
Titolare del trattamento	· nome e dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; · finalità del trattamento; · categorie di interessati e categorie di dati personali; · categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali; · trasferimenti dei dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate; · termini ultimi previsti per la cancellazione delle diverse categorie di dati (ove possibile); · descrizione generale delle misure di sicurezza tecniche e organizzative (ove possibile).
Responsabile del trattamento	· nome e dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; · categorie dei trattamenti effettuati per conto di ogni titolare del trattamento; · categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali; · trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate; · descrizione generale delle misure di sicurezza tecniche e organizzative (ove possibile).

3.8 Misure di sicurezza "adeguate"

Rispetto al Codice della *privacy* (art. 33 e allegato B), non ci sono più le misure minime di sicurezza, ma è il titolare del trattamento (e il responsabile) a dover adottare misure tecniche e organizzative "*adeguate*" al fine di "*garantire un livello di sicurezza adeguato al rischio*" del trattamento (art. 32 del reg. UE 679/2016).

Sarà, quindi, il titolare a valutare le misure necessarie, caso per caso, rispetto ad una serie di elementi, di seguito indicati:

- stato dell'arte;

- costi di attuazione;
- natura, oggetto, contesto e finalità del trattamento;
- rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

La conformità ai requisiti richiesti può essere dimostrata mediante il ricorso a meccanismi di certificazione e l'adesione a Codici di condotta.

3.9 Valutazione di impatto sulla protezione dei dati

La valutazione di impatto sulla protezione dei dati (DPIA) costituisce un ulteriore adempimento derivante dal principio introdotto della responsabilizzazione (*accountability*) dei titolari nei confronti dei trattamenti da questi effettuati (artt. 35 e 36 del reg. UE 679/2016).

La valutazione, da effettuare *ex ante* al trattamento ad opera del titolare del trattamento consultandosi con il responsabile della protezione dei dati personali, ricorre come obbligo in caso di trattamento molto rischioso per i diritti e le libertà delle persone fisiche. Ciò può derivare da vari elementi, come, ad esempio, l'uso di nuove tecnologie, ovvero in considerazione di altre caratteristiche (natura, oggetto, contesto, finalità) del trattamento.

La valutazione di impatto sulla protezione dei dati è richiesta, poi, nello specifico, nei casi seguenti:

- 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*";
- trattamento, su larga scala, di categorie particolari di dati personali o dei dati relativi a condanne penali e a reati;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Quando la valutazione di impatto indichi la sussistenza per il trattamento di un rischio elevato, nel caso in cui le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti, il titolare è tenuto a consultare l'autorità di controllo.

Contenuto minimo della valutazione di impatto sulla protezione dei dati (DPIA)

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

3.10 Violazione dei dati ("*data breach*")

Rispetto al Codice della *privacy* (art. 32-*bis*), viene prevista la notifica da parte del titolare del trattamento di ogni violazione dei dati trattati all'autorità competente entro 72 ore dal momento in cui ne venga a conoscenza (e comunque senza ingiustificato ritardo) e, in casi gravi, anche all'interessato. Tale adempimento è necessario solo se si ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (artt. 33 e 34 del reg. UE 679/2016).

4 Documenti interpretativi

Si fornisce di seguito in forma tabellare l'elenco dei documenti interpretativi e delle schede informative rilasciate sul regolamento UE 679/2016 dal Garante per la protezione dei dati personali e dal Gruppo di lavoro *ex* Articolo 29.

Linee guida ed altri documenti

Materia	**Autorità**	**Documenti**
Regolamento *privacy*	Garante per la protezione dei dati personali	· Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali (luglio 2017) · Guida al nuovo Regolamento europeo in materia di protezione dei dati personali (giugno 2016) · Scheda informativa – Regolamento 2016/679/UE: le priorità per le PA

Linee guida ed altri documenti

Materia	Autorità	Documenti
Responsabile della Protezione dei Dati (RPD)	Garante per la protezione dei dati personali	· Nuove Faq sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (15.12.2017) · Regolamento *privacy*, come scegliere il responsabile della protezione dei dati. Le prime indicazioni del Garante: necessarie competenze specifiche non attestati formali (Newsletter 15.9.2017) · *Data Protection Officer* – Scheda informativa (rispetto alle Linee guida del WP29 5.4.2017) · Schema di atto di designazione del Responsabile della Protezione dei Dati personali (RPD) ai sensi dell'art. 37 del Regolamento UE 2016/679 · Modello di comunicazione al Garante dei dati dell'RPD ai sensi dell'art. 37, par. 1, lett. a) e par. 7 del RGPD – Dati del titolare/responsabile del trattamento
	Gruppo di lavoro *ex* Articolo 29	· Linee guida sui responsabili della protezione dei dati (13.12.2016, emendate il 5.4.2017)

Linee guida ed altri documenti

Materia	Autorità	Documenti
Diritto alla portabilità dei dati	Garante per la protezione dei dati personali	· La scheda informativa del Garante (rispetto alle Linee guida del WP29 5.4.2017)
	Gruppo di lavoro *ex* Articolo 29	· Linee-guida in materia sul diritto alla portabilità dei dati (13.12.2016, emendate il 5.4.2017) · Le risposte alle domande più frequenti – FAQ (WP242 ALLEGATO)
Autorità di controllo capofila	Gruppo di lavoro *ex* Articolo 29	· Linee guida per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento (13.12.2016, emendate il 5.4.2017) · Le risposte alle domande più frequenti – FAQ (WP244 ALLEGATO)

Linee guida ed altri documenti

Materia	**Autorità**	**Documenti**
Valutazione d’impatto sulla protezione dei dati	Garante per la protezione dei dati personali	· Valutazione d’impatto sulla protezione dei dati – Scheda informativa (rispetto alle Linee guida del WP29 4.10.2017)
	Gruppo di lavoro *ex* Articolo 29	· Linee-guida concernenti valutazione impatto sulla protezione dati (4.4.2017, emendate 4.10.2017)
Processi decisionali automatizzati e profilazione	Gruppo di lavoro *ex* Articolo 29	· *Guidelines on Automated individual decision-making and Profiling for the purposes of Regula-tion* 2016/679 (3.10.2017, emendate 6.2.2018)
Notifica delle violazioni di dati personali	Gruppo di lavoro *ex* Articolo 29	· *Guidelines on Personal data breach notification under Regulation* 2016/679 (3.10.2017, emendate 6.2.2018)
Applicazione e definizione delle sanzioni amministrative	Gruppo di lavoro *ex* Articolo 29	· Linee guida riguardanti l’applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679 (3.10.2017)
Consenso	Gruppo di lavoro *ex* Articolo 29	· *Guidelines on Consent under Regulation* 2016/679 (28.11.2017)
Trasparenza	Gruppo di lavoro *ex* Articolo 29	· *Guidelines on transparency under Regulation* 2016/679
Accreditamento degli organismi di certificazione	Gruppo di lavoro *ex* Articolo 29	· *Guidelines on the accreditation of certification bodies under Regulation* (EU) 2016/679 (6.2.2018)