IL TEMA DEL MESE

MARZO 2018

LE SCADENZE

☐ **07/03/2018**

- Termine di invio telematico all'Agenzia delle Entrate della certificazione unica Cu 2018 relativa ai dipendenti, i pensionati, i collaboratori coordinati e continuativi, i lavoratori autonomi;

☐ **16/03/2018**

- Termine di versamento del saldo IVA 2017 e dell'acconto relativo all'anno 2018 (possibile differimento fino al 30 giugno 2018 con maggiorazione dello 0,40%);

☐ **16/03/2018**

- Termine di pagamento della tassa di vidimazione dei libri sociali per le società di capitali;

☐ **31/03/2018**

- Termine di consegna delle certificazioni relative ai redditi e compensi erogati nel 2017 da parte dei sostituti d'imposta (datori di lavoro e committenti);

Per l'elenco completo degli adempimenti e scadenze fiscali relativi al mese di Marzo 2018 si rinvia al sito dell'Agenzia delle Entrate al seguente link:

https://www1.agenziaentrate.gov.it/strumenti/scadenzario/main.php

IL TEMA DEL MESE

Il regolamento europeo sulla privacy (*)

A partire dal **25 maggio 2018** diventano definitivamente applicabili in via diretta in tutti i Paesi UE le disposizioni del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, alla libera circolazione di tali dati e agli adempimenti per le imprese e per le pubbliche amministrazioni.

Il Nuovo Regolamento prevede disposizioni qualitativamente e quantitativamente diverse da quelle che erano previste dal Codice della Privacy.

(*) documento a cura di Filippo Capuano

Il regolamento europeo sulla privacy

1. Premessa

A partire dal **25 maggio 2018** diventano definitivamente applicabili in via diretta in tutti i Paesi UE le disposizioni del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, alla libera circolazione di tali dati e agli adempimenti per le imprese e per le pubbliche amministrazioni.

Il provvedimento abroga la direttiva 95/46, da cui discende, ma fino a quella data rimane in vigore, in Italia, il Codice della Privacy istituito con il D.Lgs 196/2003

Il Nuovo Regolamento prevede disposizioni qualitativamente e quantitativamente diverse da quelle che erano previste dal Codice della Privacy.

Per quanto concerne le differenze qualitative si nota subito come molti adempimenti non trovano una indicazione predeterminata dalla norma, ma sono descritti nella loro finalità lasciando al titolare l'onere di completare la definizione in concreto.

La flessibilità delle norme è sicuramente un aspetto importante perché consente alle norme stesse di essere sostenibili dalle imprese, ma andrà però soppesata con il sistema sanzionatorio che colpisce anche ogni minima inosservanza (capo VII articoli da 77 a 84). Le sanzioni amministrative previste potranno arrivare fino a 20 milioni di euro o al 4% del fatturato annuo globale.

Le sanzioni dovranno assicurare la non ripetibilità dell'illecito e saranno commisurate alla numerosità dei dati trattati e proporzionali alla dimensione dell'azienda. Le sanzioni penali saranno determinate dalle legislazioni nazionali, nel rispetto del principio **"ne bis in idem"** (non due volte per la stessa cosa).

La legge delega italiana 163/2017 all'articolo 13 prevede che debba essere adeguato, nell'ambito delle modifiche al codice del D.Lgs 196/2003, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679, con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

2. Il Regolamento in sintesi

Disposizioni generali (articoli 1 -4)	Viene spiegato il campo di applicazione (anche territoriale) e illustrato il vocabolario
Principi (articoli 5-11)	Vengono illustrate le condizioni alle quali si possono trattare i dati (obbligo per soggetto privato o PA – consenso e caratteristiche, necessità o meno)

Diritti (articoli 12-23)	Vengono elencate le prerogative dell'interessato (pretese – diritti - trasparenza e accesso – esattezza del dato – oblio – profilazione mitigata – limitazione)
Principali attori protagonisti (articoli 24-31)	Vengono indicati ruoli e responsabilità (titolare – contitolare – rappresentante – responsabile trattamento – autorizzato – registri attività)
Sicurezza (articoli 32-39)	Vengono indicati i sistemi delle precauzioni da adottare – analisi dei rischi e misure – valutazione d'impatto e consultazione preventiva – responsabile protezione dei dati (DPO/RPD)
Sistema di Regolazione (articoli 40 -43)	Viene trattata una regolazione collettiva – codici di condotta – certificazione della qualità di prodotti e servizi – sistemi ammessi e benefici
Trasferimento dati all'estero (articoli 44 -50)	Vengono trattati modalità trasferimento e deroghe
Autorità di controllo indipendenti (articoli 51-59)	Vengono disciplinati gli aspetti relativi a Competenza – composizione - indipendenza – poteri – rapporti reciproci - Autorità (in Italia il Garante)
Cooperazione e coerenza (articoli 60-76)	Viene regolata la cooperazione tra autorità di controllo
Mezzi di ricorso, responsabilità e sanzioni (articoli 77-84)	Vengono trattate la responsabilità civile e le sanzioni amministrative
Disposizioni relative a specifiche situazioni di trattamento (articoli 85-91)	Viene rinviata agli stati nazionali la disciplina di alcuni settori (stampa, chiese, rapporti di lavoro, sistema statistico, ecc.)
Atti delegati e atti di esecuzione - Disposizioni finali (articoli 92-99)	Sono dettate norme su deleghe – tempi di applicazione e entrata in vigore

3. Disposizioni generali e definizioni

Tra le definizioni contenute nell'articolo 4 del Regolamento, una delle fondamentali è quella di «**dato personale**», definito come 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.

Viene definito poi il «**trattamento**»: qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.

Sono tali la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

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

L'articola 4 elenca inoltre tutte le altre definizioni la cui conoscenza è prerequisito necessario per poter comprendere l'intero Regolamento e come devono essere classificati e organizzati i dati, come deve avvenire il trattamento e qual è il ruolo dei soggetti coinvolti.

Si tratta delle nozioni di limitazione di trattamento – profilazione – pseudonimizzazione – archivio - responsabile del trattamento – destinatario – terzo - consenso dell'interessato - violazione dei dati personali - dati genetici - dati biometrici - dati relativi alla salute - stabilimento principale – rappresentante – impresa - gruppo imprenditoriale - norme vincolanti d'impresa - autorità di controllo - autorità di controllo interessata - trattamento transfrontaliero - obiezione pertinente e motivata - servizio della società dell'informazione - organizzazione internazionale.

4. Valutazione del rispetto dei principi privacy

L'articolo 5, al paragrafo 1, elenca i principi applicabili al trattamento dei dati personali, riprendendo in parte quelli già enunciati nella Direttiva 95/46/CE (liceità e correttezza) e specificando più nel dettaglio il contenuto di altri (trasparenza, minimizzazione, esattezza, limitazione di conservazione, integrità e riservatezza).

Il paragrafo 2 del medesimo articolo introduce il principio di responsabilizzazione, così espresso: "*il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione)*".

La portata generale del principio rappresenta una delle chiavi di lettura dell'intero Regolamento. Per responsabilizzazione, infatti, deve intendersi la presa di coscienza attiva, da parte dei titolari del trattamento, della necessità di una protezione dei dati personali degli interessati e della conseguente conformità del trattamento alla nuova disciplina.

In sostanza, il principio di responsabilizzazione richiede un diverso approccio applicativo delle disposizioni del Regolamento rispetto alla Direttiva, "ribaltando" sui titolari del trattamento un obbligo di autovalutazione rispetto al trattamento effettuato, alla tipologia dei dati personali trattati, ai rischi derivanti da tale trattamento e, soprattutto, rispetto all'adeguatezza delle misure tecniche e organizzative predisposte affinché il trattamento sia conforme al Regolamento.

5. Diritti dell'interessato: informativa privacy e consenso

L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti. Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile. Deve essere utilizzato un linguaggio chiaro e semplice e per i minori devono essere previste informative idonee.

L'informativa è data, in linea di principio, per iscritto o anche in formato elettronico (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).

Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea. Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie, cosi come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).

Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito». Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate. Il consenso potrà essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi. I fornitori di servizi Internet e i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.

6. L'esercizio dei Diritti dell'Interessato

L'articolo 12 del "Nuovo Regolamento" disciplina in linea generale le modalità per l'esercizio di tutti i diritti in capo all'interessato. La normativa prevede che il titolare del trattamento deve rispondere all'interessato delle richieste relative ai suoi diritti entro il termine di 1 mese (termine estendibile sino a 3 mesi, in casi di particolare complessità).

Rispetto alla previgente normativa, il Nuovo Regolamento ha introdotto l'onere in capo al titolare di "*valutare la complessità del riscontro all'interessato, al fine di stabilire l'ammontare dell'eventuale contributo da richiedere all'interessato*". Questo, però, vale solo nei casi in cui le richieste dell'interessato siano manifestatamente infondate e ripetitive.

Inoltre, il Legislatore Comunitario ha previsto l'obbligo - gravante sul titolare - di rispondere regolarmente in forma scritta alle richieste dell'interessato, anche attraverso strumenti elettronici che ne favoriscano l'accessibilità. Le informazioni richieste potranno esser concesse all'interessato in forma orale solo nel caso in cui sia lo stesso a farne esplicita richiesta.

L'articolo 15 primo comma definisce il diritto di accesso dell'interessato al trattamento di dati personali come quel diritto di richiedere e ottenere dal titolare del trattamento - senza "giustificato ritardo" - la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano. Pertanto, in termini più generali, l'interessato ha il diritto di richiedere al titolare del trattamento di prendere visione o estrarre copia dei vari tipi di documenti a lui riferibili, in applicazione del più generale principio di trasparenza del trattamento dei dati personali.

Il diritto di accesso ai dati si fonda, inoltre, sul principio di gratuità e pertanto l'interessato potrà ricevere le informazioni senza pagare alcuna somma a titolo remunerativo. Resta ferma ad ogni modo la possibilità, per il titolare, di addebitare i costi all'interessato in alcuni particolari casi, ovvero, ad esempio, ove lo stesso richieda copie di documenti.

Sul punto si precisa che è molto probabile che l'Autorità Garante intenda valutare l'opportunità di definire eventuali linee-guida specifiche quanto alla definizione di un eventuale contributo spese da parte degli interessati, cosa che invece il Regolamento rimette al titolare del trattamento.

Nel caso in cui l'interessato richieda di accedere ai propri dati, il titolare del trattamento ha l'onere di fornire all'interessato sia una copia dei dati personali oggetto di trattamento che lo riguardano sia - come previsto dall'articolo 15 - ulteriori informazioni. Si tratta di informazioni che riguardano le finalità del trattamento, le categorie di dati personali trattati, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, la possibilità per l'interessato di esercitare il diritto di rettifica, alla cancellazione, alla limitazione del trattamento, e il diritto di opposizione al trattamento.

Inoltre, rispetto alla precedente normativa privacy, 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.

Oltre a ciò la normativa europea prevede che, ove l'interessato abbia presentato la richiesta di accesso mediante mezzi elettronici, le informazioni devono essere fornite in un formato elettronico "di uso comune", salvo diverse indicazioni.

Infine, è compito del titolare del trattamento verificare l'identità dell'interessato che richiede l'accesso ai suoi dati, adottando tutte le misure necessarie per evitare che soggetti terzi possano abusivamente esser messi a conoscenza dei dati trattati.

Come noto, il "diritto di accesso" è uno dei principi portanti in tema di privacy; la previgente disciplina (articolo 12 della Direttiva 95/46/CE) prevedeva che il soggetto interessato poteva ottenere liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi la conferma dell'esistenza o meno di un trattamento. Il Legislatore Comunitario, volendo ampliare tutta la disciplina relativa alla trasparenza ed agli obblighi informativi in tema di privacy, introduce così un "nuovo" diritto di accesso che, rispetto alla normativa passata, si rafforza e si dettaglia, tanto da acquistare il ruolo di diritto fondamentale delle persone fisiche, previsto al fine ultimo di cristallizzare una garanzia agli interessati a tutela della veridicità dei propri dati.

Inoltre, oltre al rispetto delle prescrizioni relative alla modalità di esercizio di questo e degli altri diritti, i titolari possono consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

All'articolo 17 del Nuovo Regolamento il Legislatore Comunitario ha previsto l'esistenza di un diritto in capo all'interessato ad ottenere la cancellazione dei dati oggetto di trattamento e ad esso riferiti o riferibili, assicurando pertanto il "diritto all'oblio".

Infine, tra i diritti annoverati in tema di privacy, il Legislatore Comunitario all'articolo 21 ha disciplinato inoltre il c.d. "Diritto di opposizione", il quale per definizione consente all'interessato di opporsi "*in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano*". In virtù dell'esercizio di tale diritto, il titolare potrà continuare a trattare i dati in suo possesso solo ove dimostri "*l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria*".

7. Adempimento degli obblighi privacy in caso di Profilazione

Il Regolamento definisce come «profilazione» qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati 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 della persona.

Inoltre, per i trattamenti che comportano attività di profilazione o di marketing diretto, la norma comunitaria prevede che: "*qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non potranno più essere oggetto di trattamento per tali finalità*".

8. Progettazione nel rispetto della Privacy by Design e Privacy by Default

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili, cioè sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento. Si tratta di una importante novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali. Il tutto deve però avvenire nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Primo fra tali criteri, ripreso dall'espressione inglese "data protection by default and by design", è la necessità di impostare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento vero e proprio, e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Quindi per Privacy by Design si intende, in breve, la necessità di tutelare il dato sin dalla progettazione di sistemi informatici e informativi aziendali che ne prevedano l'utilizzo.

Il concetto di Privacy by Default intende invece sottolineare la necessità della tutela delle persone fisiche come impostazione predefinita, e quindi il Titolare del Trattamento deve mettere in atto misure tecniche ed organizzative adeguate affinché i dati personali siano trattati per impostazione predefinita sin da subito esclusivamente solo per le necessità che derivano da ogni singolo trattamento.

9. Principali figure richieste dal Regolamento

La complessità della protezione dei dati, in una era sempre più tecnologica, richiede varie figure con diversi compiti: alcune sono espressamente previste nel Regolamento, mentre altre derivano direttamente dalle necessità che le aziende riscontrano dalla necessità di gestire correttamente i dati.

Il titolare del trattamento è soggetto agli obblighi/responsabilità elencati nell'articolo 24:

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

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

3. L'adesione ai codici di condotta indicati all'articolo 40 o a un meccanismo di certificazione indicato all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Poiché l'attività di protezione delle persone muta in relazione ai luoghi e ai tempi, il principio di responsabilizzazione comporta che il titolare dimostri di essersi continuativamente preoccupato di adeguare nello scorrere del tempo le misure di risposta adeguata.

Il Responsabile del Trattamento è invece la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del Titolare del Trattamento.

Il regolamento fissa più dettagliatamente 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'articolo 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti", quali, in particolare, la natura, durata e 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.

E' consentita la nomina di sub-responsabili del trattamento, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario che però 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.

Sono infine previsti obblighi specifici in capo ai responsabili del trattamento, in particolare: la tenuta del registro di tutte le categorie dei trattamenti svolti per conto di un titolare (articolo 30, paragrafo 2), l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (articolo 32).

Il rappresentante del titolare o del responsabile del trattamento è invece il soggetto che il titolare o il responsabile non stabilito nell'Ue dovrà designare nel territorio della Ue quando ricorrono le condizioni previste dall'articolo 27, paragrafo 3. Il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato.

La figura dell'incaricato del trattamento già prevista dal Codice della privacy (96/2003) come "*la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile*", con il Regolamento Ue non è più espressamente prevista. Ciò non significa però che questa figura non sia importante nell'organizzazione aziendale per quanto concerne il trattamento dei dati. E' quindi possibile ed anzi auspicabile la nomina degli incaricati/autorizzati al trattamento dei dati nei termini noti agli operatori italiani, in particolare riguardo ai requisiti oggettivi (ad esempio nel quadro delle misure di sicurezza che il titolare del trattamento è tenuto ad adottare).

Il Regolamento (articolo 29) prevede inoltre per il titolare del trattamento *l'obbligo di formare gli addetti autorizzati al trattamento dei dati*. Chiunque agisce sotto l'autorità del titolare del trattamento o del responsabile, che abbia accesso ai dati.

Infine, il regolamento disciplina la contitolarità del trattamento 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, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.

10. Il Responsabile della Protezione dei Dati (RPD/DPO)

Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda articolo 39), essendo fializzata a facilitare l'attuazione del regolamento da parte del titolare/ responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'articolo 35. La sua designazione è obbligatoria

in alcuni casi (si veda articolo 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa fiura (indipendenza, autorevolezza, competenze manageriali: si vedano articoli 38 e 39).

I soggetti obbligati a designare un responsabile della protezione dei dati "RPD" sono:

- amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;
- tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un RPD è comunque possibile una nomina su base volontaria. Un gruppo di imprese o soggetti pubblici possono nominare un unico RPD.

Il responsabile della protezione dei dati dovrà, in particolare:

- sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA- Data Protection Impact Assessment);
- informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;
- supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

Il RPD, anche secondo quanto chiarito attraverso alcune linee guida di recente pubblicazione, disponibili sul sito del Garante, non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dati. Spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento. Il RPD, tuttavia, assume responsabilità contrattuali nei confronti del titolare/responsabile del trattamento.

11. Il Registro delle attività di trattamento (Registro Privacy)

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti, ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati nell'articolo 30.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo, è opportuno che tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, prendano in considerazione l'adozione di tale registro e, in ogni caso, compiano un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

12. Definizione delle misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento in questo senso, la lista del paragrafo 1 dell'articolo 32 è una lista aperta e non esaustiva dove il titolare e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate che comprendono:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre, i pericoli incombenti sulla privacy delle persone sono costantemente in aumento a causa del progresso tecnologico che può, da un lato, compromettere la sicurezza dei dati che vengono conservati e, dall'altro, consentire ai titolari del trattamento di aggregare informazioni acquisite su uno stesso individuo senza che il soggetto cui esse appartengono sia consapevole di poter essere identificato o di rendersi identificabile per il fatto di averle conferite. Il Regolamento Europeo ha introdotto una nuova soluzione che favorisce la tutela dell'individuo e dei suoi dati personali: si tratta della pseudonimizzazione, cioè "*il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e*

organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile"

Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex articolo 33 D.Lgs 196/2003) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del regolamento.

Si richiama inoltre l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Come indicato dal nuovo Regolamento Europeo, "*l'adesione a un codice di condotta o a un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare la conformità ai requisiti di sicurezza*".

Esempio: schema di organizzazione per la sicurezza

procedura	**obiettivi**
Politiche di sicurezza	Fornire le direttive di gestione ed il supporto per le informazioni di sicurezza in azienda.
Sicurezza organizzativa	Controllare la sicurezza delle informazioni. Garantire il mantenimento della sicurezza e della facilità dei processi organizzativi delle informazioni anche quando eccedono le terze parti. Monitorare la sicurezza delle informazioni quando la responsabilità dell'elaborazione dell'informazione è stata conferita in out source.
Controllo e classificazione dei beni (hardware and software)	Mantenere la protezione dell'assetto organizzativo e garantire che l'assetto delle informazioni riceva un appropriato livello di protezione.
Sicurezza del personale	Ridurre i rischi di errore, di furto, di frode o di abuso da parte degli operatori. Accertarsi che gli utenti siano informati delle possibili minacce e preoccupazioni sulla sicurezza delle informazioni e riescano a

	sostenere la politica della società sulla sicurezza nel corso del loro normale lavoro. Eseguire la formazione finalizzata a minimizzare i danni degli avvenimenti e delle disfunzioni di sicurezza ed imparare a gestire tali avvenimenti.
Sicurezza fisica e ambientale	Impedire l'accesso, il danneggiamento e l'interferenza dei non autorizzati all'interno del flusso delle informazioni del business. Impedire perdita, danni o l'assetto del sistema e la interruzione delle attività economiche. Impedire la manomissione o il furto delle informazioni.
Gestione di comunicazioni e operazioni	Accertarsi del corretto funzionamento e facilità di elaborazione dell'informazione. Minimizzare il rischio di guasti dei sistemi. Proteggere l'integrità dei software e delle informazioni. Mantenere l'integrità e la validità dei processi di elaborazione dell'informazione e della comunicazione. Garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture a supporto. Prevenire danni ai beni e le interruzioni alle attività economiche. Impedire perdita, modifica o abuso delle informazioni scambiate fra le organizzazioni.
Sviluppo e manutenzione dei sistemi – system development and maintenance	Accertare che la sicurezza sia stata costruita all'interno delle operazioni di sistema: - per impedire la perdita, la modifica o il cattivo utilizzo dei dati dell'utente all'interno dei sistemi di applicazione; - per proteggere la riservatezza, autenticità e l'integrità delle informazioni; - per accertarsi che le attività di progetto e supporto alle attività siano condotte in modo

	sicuro e per mantenere la sicurezza del software e dei dati di sistema.
Gestione continuità operativa – business continuity management	Capacità di neutralizzare le interruzioni alle attività economiche ed ai processi critici degli affari, nonostante il manifestarsi di incidenti e di eventi catastrofici.
Adeguatezza – compliance	Evitare il non rispetto delle leggi civili, penali e di qualsiasi requisito di sicurezza. Elevare l'efficacia e minimizzare l'interferenza da/per il processo di verifica del sistema.

13. La costruzione del sistema di Gestione Privacy

In linea generale ogni organizzazione deve:

- valutare attentamente la propria situazione specifica e il contesto in cui opera;
- identificare le caratteristiche del trattamento effettuate;
- adottare misure tecnico-organizzative che garantiscano un livello di protezione adeguato tutelando fin dall'inizio i diritti dell'interessato;
- costruire un organigramma dei soggetti che devono trattare i dati;
- incaricare e autorizzarre i soggetti preposti al trattamento;
- istruire il personale interno incaricato;
- verificare le clausole dei contratti stipulati con i propri fornitori di servizi per assicurarsi che le operazioni di trattamento avvengano secondo la corretta attribuzione di ruoli e responsabilità, come richiesto dal Regolamento;
- predisporre procedure per rispondere alle richieste degli "interessati" in merito ai propri dati e conservare tutta la documentazione relativa, così da poterla esibire in caso di richiesta dell'Autorità preposta;
- conservare la documentazione attestante la liceità del trattamento effettuato;
- organizzarsi per rispondere alle eventuali richieste dell'Autorità;
- definire metodi documentati per gestire eventuali violazioni dei dati;
- monitorare costantemente lo "stato di salute" dei propri processi e dei trattamenti su dati personali, anche per identificare possibili manomissioni o intrusioni;
- recepire prontamente gli aggiornamenti normativi che dovessero man mano intervenire.

14. Violazione dei dati personali (Data Breach) e comunicazioni e al Garante

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

Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine, ecc.), oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati, oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato (ad esempio, se il numero delle persone coinvolte è elevato). In questo ultimo caso, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio, tramite un'inserzione su un quotidiano o una comunicazione sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

A partire dal 25 maggio 2018, quindi, tutti i titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo".

I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli articoli 33 e 34 del regolamento. Su questo e su tutta la disciplina in materia, dovranno essere elaborate e pubblicate linee-guida specifiche.

Si ricorda, inoltre, che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico

(http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835), che intende rielaborare, al fine di renderlo utilizzabile da tutti i titolari di trattamento, quanto prevede il regolamento.

Si segnalano poi, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali recentemente pubblicate e attualmente in consultazione pubblica (Http://ec.europa.eu/newsroom/document.cfm?doc_id=47741).

15. Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (ad es. a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio.

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

Le linee-guida (http://www.garanteprivacy.it/DPIA) del Gruppo di Lavoro ex art. 29 (WP29 - Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD - Garante europeo della protezione dei dati- nonché da un rappresentante della Commissione) offrono alcuni chiarimenti sul punto: in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all'articolo 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

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

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

Ci possono essere casi, infine, in cui la valutazione di impatto privacy non è sufficiente. Se, infatti dalla valutazione d'impatto emergesse che il rischio per la protezione dei dati non può essere ragionevolmente attenuato mediante l'uso delle

tecnologie disponibili e/o per gli elevati costi di attuazione, è necessario consultare preventivamente l'autorità Garante prima dell'inizio dell'attività di controllo.

16. Adozione di Codici di Condotta e certificazione del Sistema

Il regolamento europeo incoraggia l'adozione di codici di condotta e l'utilizzo dello strumento delle certificazioni per attenuare il rischio connesso al trattamento dei dati personali e per contribuire alla corretta applicazione del regolamento, in funzione delle specificità dei vari settori e delle esigenze specifiche delle micro, piccole e medie imprese.

L'importanza dei codici di condotta nel nuovo impianto normativo per la protezione dei dati personali è data dal fatto che, con l'entrata in vigore del Regolamento, l'onere della prova di aver attuato le misure organizzative e di sicurezza adeguate alla particolare tipologia di dati e di trattamento effettuato sarà in capo al titolare e al responsabile del trattamento.

In tale contesto, i codici di condotta e i meccanismi di certificazione potranno assumere un ruolo importante, in quanto, ai sensi dell'articolo 24, terzo comma, del Regolamento potranno essere utilizzati come elementi per dimostrare il rispetto degli obblighi del titolare del trattamento.

Il Regolamento promuove quindi il ricorso a codici di condotta da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati ed eventualmente della Commissione Europea (nel caso dell'approvazione da parte della Commissione il codice di condotta avrà applicazione nell'intera Ue). Il titolare potrà far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi. La certificazione potrà essere rilasciata da un soggetto abilitato oppure dall'Autorità di protezione dei dati. L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

17. I contratti per il trasferimento di dati all'estero

Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o verso organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.

Come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione europea, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti.

In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).

Il trasferimento o la comunicazione di dati personali di un cittadino dell'Ue ad autorità giudiziarie o amministrative di Paesi terzi potranno avvenire solo sulla base di accordi internazionali di mutua assistenza giudiziaria o attraverso strumenti analoghi.

18. Autorità di controllo e Cooperazione

Ogni Stato dell'Unione Europea deve avere una o più Autorità di controllo, autonoma e indipendente (il Garante Privacy in Italia). Oltre a quanto previsto dal Regolamento, il diritto interno degli stati membri può prevedere per l'Autorità di controllo poteri ulteriori.

L'esercizio dei poteri del Garante è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale ed il giusto processo.

I poteri attribuiti al Garante dal Regolamento sono poteri d'indagine, poteri correttivi, poteri autorizzativi e consultivi.

I poteri d'indagine hanno una finalità preventiva; i poteri correttivi hanno finalità repressiva, mentre i poteri autorizzativi mirano alla verifica di requisiti particolari per poter procedere al trattamento.

E' previsto il principio "one stop shop" che significa che il titolare del trattamento può rivolgersi all'autorità Garante del Paese in cui è stabilito, la quale opererà come autorità capofila per tutte le attività svolte in tutti i Paesi della Unione Europea.

L'Autorità capofila deve cooperare con le altre autorità interessate ed è competente per l'adozione di decisioni vincolanti.

19. Reclami e Ricorsi al Garante Privacy

Il Regolamento prevede due forme di tutela dell'interessato, amministrativa e giurisdizionale:

- reclamo (ex articolo 77)
- ricorso giurisdizionale nei confronti dell'autorità di controllo (ex articolo 78) e nei confronti del titolare e/o del responsabile del trattamento (ex articolo 79).

Gli interessati hanno inoltre il diritto di dare mandato ad un organismo o organizzazione o associazione, attiva nel settore della protezione dei dati, che li rappresenti e che proponga reclamo per loro conto. Tali associazioni possono, se la

legislazione dello Stato membro lo prevede, agire anche autonomamente, proponendo il reclamo all'autorità di controllo competente o i ricorsi giurisdizionali sopra descritti, qualora ritengano che i diritti di cui un interessato gode a norma del Regolamento siano stati violati nell'ambito di un trattamento.

Ogni autorità di controllo provvede, se ne ricorrono i presupposti, ad infliggere sanzioni amministrative pecuniarie effettive, proporzionate e dissuasive.

Tali sanzioni devono essere circostanziate il più possibile e vanno a sommarsi all'esecuzione di tutte quelle misure ritenute idonee e imposte dall'autorità di controllo stessa nell'ambito dei suoi poteri di indagine e correzione.

Nell'articolo 83 del Regolamento vi è un esaustivo ma non tassativo elenco di elementi da tenere in considerazione nel momento in cui si infligge una sanzione amministrativa e ne viene si fissato l'ammontare. Sono poi previsti i casi in cui, a seguito di una violazione, si può comminare una sanzione fino a 10.000.000 di euro e quelli in cui la sanzione può raggiungere addirittura i 20.000.000 di euro.

In particolare tale ultimo e più gravoso provvedimento viene adottato qualora non vengano rispettati i principi base del trattamento, comprese le condizioni relative al consenso, ovvero i diritti fondamentali di cui gode l'interessato previsti dagli articoli da 12 a 22 e quando vengono violate le disposizioni circa i trasferimenti di dati personali a un destinatario in un paese terzo.

E’ comunque demandato ai singoli Stati membri stabilire le norme relative alle altre sanzioni per le violazioni del Regolamento, in particolare per quei casi in cui non sono già previste le sanzioni amministrative pecuniarie sopra citate. Gli Stati devono quindi adottare tutti i provvedimenti necessari per assicurare l'applicazione di tali sanzioni che devono essere effettive, proporzionate e dissuasive.

In un'ottica di armonizzazione e di controllo, ogni paese membro dovrà notificare alla Commissione europea le disposizioni di legge adottate inerenti le sanzioni entro il 25 maggio 2018, comunicando in modo tempestivo ogni successiva modifica.

20. Il periodo transitorio dal Codice Privacy (D.Lgs 196/2003) al Regolamento 2016/679

I titolari del trattamento dovranno allineare i loro sistemi e le loro prassi al nuovo ordinamento.

Dovranno essere verificate tutte le attuali procedure in tema di trattamento dati personali e dovrà essere redatta una relazione sullo stato di attuazione degli adempimenti di legge, finalizzata alla predisposizione di un programma di

adeguamento coerente con la normativa e con le reali necessità dell'azienda/organismo, anche in termini di dimensione qualitativa e quantitativa del trattamento.

Non tutti gli adempimenti previsti dal regolamento sono obbligatori per ogni titolare, ma dipendono da specifici parametri che andranno valutati caso per caso.

Tutti i provvedimenti del Garante Privacy che non sono in contrasto con il regolamento rimarranno in vigore (ad esempio, le norme in materia di videosorveglianza).