La privacy in chiave europea guarda ai modelli “231”

Sommario:

I. Le linee-guida del WP29 nella loro versione aggiornata ad ottobre 2017; ***II.*** *Autorizzata una banca dati privata per prevenire condotte fraudolente nei rapporti contrattuali; III. Le Nuove FAQ sul Responsabile della Protezione dei dati (RPD) in ambito pubblico; IV. La Commissione Europea pubblica orientamenti sulle nuove norme in materia di protezione dei dati; V. Le modifiche introdotte con la legge di Bilancio 2018.*

I. Le linee-guida del WP29 nella loro versione aggiornata ad ottobre 2017.

Ad ottobre 2017 è stata rilasciata una versione aggiornata delle linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248), le stesse precisano quando debba ritenersi obbligatoria una valutazione di impatto (oltre ai casi espressamente indicati dal Regolamento all'art. 35[1]), 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[2].
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.

[1] L’art. 35 del Regolamento stabilisce che il titolare, prima di avviare un trattamento che prevede l’uso di nuove tecnologie e considerati la natura, l’oggetto, il contesto e le finalità, debba operare una valutazione dell’impatto dei trattamenti previsti sulla protezione dei dati personali.
Tuttavia, lo stesso articolo, al par. 3, prevede anche che la valutazione d’impatto debba essere richiesta nei seguenti casi:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all’articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all’articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

[2] http://www.garanteprivacy.it/DPIA.

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 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (*data protection by design*) di qualsiasi trattamento[3].

II. Autorizzata una banca dati privata per prevenire condotte fraudolente nei rapporti contrattuali

Il Garante privacy con un provvedimento del 30 novembre 2017[4] ha autorizzato un'associazione di categoria (nel caso di specie, rappresentativa del 95% circa delle imprese operanti nel settore dell'autonoleggio a breve e lungo termine) a costituire una banca dati volta a contrastare anomalie e condotte patologiche nei rapporti contrattuali.
Nella banca dati, alimentata e consultabile dalle imprese associate, potranno confluire vari dati relativi al rapporto con la clientela, ad esclusione di dati sensibili e giudiziari e di soggetti terzi.
Per evitare iscrizioni ingiustificate, il Garante ha previsto che la registrazione nel database dati dovrà avvenire solo al verificarsi di più condizioni (irreperibilità del cliente, decorrenza di almeno 30 giorni dall'inadempimento, stipula di altri contratti similari nei 6 mesi precedenti). Vengono inoltre previsti elevati standard di sicurezza, che impongono la separazione fisica della nuova banca dalle altre gestite dall'associazione, nonché l'accesso al sistema, basato su procedure di *strong authentication*, solo tramite canali criptati e su connessioni sicure.
Infine è previsto che titolare della banca dati sia la stessa associazione di categoria, sulla quale graverà l'onere di fornire idonea informativa agli interessati, per il tramite delle stesse società di autonoleggio; queste ultime, tassativamente individuate, potranno partecipare al sistema in qualità di autonomi titolari dei dati personali raccolti in fase di stipula dei contratti di autonoleggio. I dati censiti potranno essere utilizzati dalle società partecipanti esclusivamente nei limiti delle finalità sopra indicate e con le modalità stabilite nelle apposite linee-guida veicolate dall'associazione.

III. Le Nuove FAQ sul Responsabile della Protezione dei dati (RPD) in ambito pubblico.

In data 15 dicembre 2017 il Garante per la protezione dei dati personali ha pubblicato un elenco di nuove FAQ (*Frequently Asked Questions*) in materia di Responsabile dei dati (*RPD, o DPO - Data Protection Officers*) in ambito pubblico[5].
Le FAQ rispondono alle principali richieste di chiarimento che le pubbliche

[3] http://194.242.234.211/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.
[4] Cfr. doc. web n. 7355034, Registro dei provvedimenti n. 502 del 30 novembre 2017.
[5] Le stesse devono intendersi in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle linee guida sul RPD adottate il 13 dicembre 2016 e nella versione emendata in data 5 aprile 2017.

amministrazioni hanno rivolto al Garante nell'ambito degli incontri effettuati a partire dal mese di giugno. Il documento chiarisce, in primo luogo, quali siano gli enti pubblici tenuti alla designazione del RPD e indica come, in ragione dei compiti assegnati a questa nuova figura dal Regolamento, essa sia da individuarsi in un dirigente o in un funzionario di elevata professionalità, che possa svolgere i propri compiti con adeguate garanzie di indipendenza e autonomia e possa comunque riportare direttamente al vertice dell'organizzazione[6]. Va ricordato infatti che il Responsabile della protezione dati adotta atti a rilevanza interna (pareri nei confronti del vertice dell'ente) ed esterna (comunicazioni agli interessati in relazione all'esercizio dei diritti e al Garante, con il quale è tenuto a cooperare).
Quanto ai requisiti necessari per svolgere la funzione di RPD il Garante chiarisce ancora una volta che il possesso di una specifica certificazione non deve essere considerato come abilitazione all'esercizio di tale ruolo e che spetta al titolare e al responsabile valutare il possesso dei requisiti professionali richiesti dal Regolamento.
Nelle FAQ si forniscono inoltre chiarimenti sulle procedure di designazione e sulle comunicazioni da inviare al Garante, per le quali sono stati messi a disposizione appositi modelli.
Di seguito si riportano integralmente le nuove FAQ adottate dal Garante:

1. Quali sono i soggetti tenuti alla designazione del RPD, ai sensi dell'art. 37, par. 1, lett. a), del RGPD?

L'art. 37, par. 1, lett. a), del RGPD prevede che i titolari e i responsabili del trattamento designino un RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali».
Il RGPD non fornisce la definizione di "autorità pubblica" o "organismo pubblico" e, come chiarito anche nelle Linee guida adottate in materia dal Gruppo Art. 29 (di seguito Linee guida), ne rimette l'individuazione al diritto nazionale applicabile[7].
Allo stato, in ambito pubblico, devono ritenersi tenuti alla designazione di un RPD i soggetti che oggi ricadono nell'ambito di applicazione degli artt. 18 - 22 del Codice, che stabiliscono le regole generali per i trattamenti effettuati dai soggetti pubblici (ad esempio, le amministrazioni dello Stato, anche con ordinamento autonomo, gli enti pubblici non economici nazionali, regionali e locali, le Regioni e gli enti locali, le università, le Camere di commercio, industria, artigianato e agricoltura, le aziende del Servizio sanitario nazionale, le autorità indipendenti ecc.).
Occorre, comunque, considerare che, nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), può risultare comunque fortemente raccomandato, ancorché non obbligatorio, procedere alla designazione di un RPD. In ogni caso, qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in

[6] Il documento specifica anche che non può essere designato più di un RPD per ogni titolare/responsabile il quale, se necessario, in base alla complessità dell'organizzazione, potrà eventualmente avvalersi di propri "referenti", che potrebbero svolgere un ruolo di supporto e raccordo, sulla base di precise istruzioni dell'RPD.
[7] Cfr. al riguardo il par. 2.1.1., pag. 6, delle Linee guida sui responsabili della protezione dei dati (RPD) adottate dal Gruppo Art. 29 il 13 dicembre 2016 ed emendate il 5 aprile 2017 (WP243 rev. 01), disponibili sul sito istituzionale dell'Autorità (doc. web n. 5930287).

termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria[8].

2. Nel caso in cui il RPD sia un dipendente dell'autorità pubblica o dell'organismo pubblico, quale qualifica deve avere?

Il RGPD non fornisce specifiche indicazioni al riguardo. È opportuno, in primo luogo, valutare se il complesso dei compiti assegnati al RPD - aventi rilevanza interna (consulenza, pareri, sorveglianza sul rispetto delle disposizioni) ed esterna (cooperazione con l'autorità di controllo e contatto con gli interessati in relazione all'esercizio dei propri diritti) - siano (o meno) compatibili con le mansioni ordinariamente affidate ai dipendenti con qualifica non dirigenziale.

In merito, l'art. 38, par. 3, del RGPD fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione. In particolare, occorre assicurare che il RPD "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti". Il considerando 97 aggiunge che i RPD "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente". Ciò significa, come chiarito nelle Linee guida, che «il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati».

Inoltre, sempre ai sensi dell'art. 38, par. 3, del RGPD, il RPD «riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento». Tale rapporto diretto garantisce, in particolare, che il vertice amministrativo venga a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nell'esercizio delle funzioni di informazione e consulenza a favore del titolare o del responsabile.

Alla luce delle considerazioni di cui sopra, nel caso in cui si opti per un RPD interno, sarebbe quindi in linea di massima preferibile che, ove la struttura organizzativa lo consenta e tenendo conto della complessità dei trattamenti, la designazione sia conferita a un dirigente ovvero a un funzionario di alta professionalità, che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione.

3. Quali certificazioni risultano idonee a legittimare il RPD nell'esercizio delle sue funzioni, ai sensi degli artt. 42 e 43 del RGPD?

Come accade nei settori delle cosiddette "professioni non regolamentate", si sono diffusi schemi proprietari di certificazione volontaria delle competenze professionali effettuate da appositi enti certificatori. Tali certificazioni (che non

---

[8] Anche in caso di assenza del requisito soggettivo previsto dall'art. 37, par. 1, lett. a), del RGPD, il titolare o il responsabile del trattamento sono comunque tenuti alla designazione del RPD, ai sensi di quanto previsto dall'art. 37, par. 1, lett. b) e c), nel caso in cui le attività principali consistano:
- in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
- nel trattamento su larga scala di categorie di dati personali di cui all'art. 9 del RGPD o dei dati relativi alle condanne penali e a reati di cui all'art. 10 del RGPD.

Con riferimento all'interpretazione delle espressioni «attività principali», «larga scala» e «monitoraggio regolare e sistematico» vedasi quanto riportato nelle Linee guida.

rientrano tra quelle disciplinate dall'art. 42 del RGPD) sono rilasciate anche all'esito della partecipazione ad attività formative e al controllo dell'apprendimento.
Esse, pur rappresentando, al pari di altri titoli, un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una "abilitazione" allo svolgimento del ruolo del RPD né, allo stato, sono idonee a sostituire il giudizio rimesso alle PP.AA. nella valutazione dei requisiti necessari al RPD per svolgere i compiti previsti dall'art. 39 del RGPD[9].

4. Con quale atto formale deve essere designato il RPD?
Il RGPD prevede all'art. 37, par. 1, che il titolare e il responsabile del trattamento designino il RPD; da ciò deriva, quindi, che l'atto di designazione è parte costitutiva dell'adempimento.
Nel caso in cui la scelta del RPD ricada su una professionalità interna all'ente, occorre formalizzare un apposito atto di designazione a "Responsabile per la protezione dei dati". In caso, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante dell'apposito contratto di servizi redatto in base a quanto previsto dall'art. 37 del RGPD[10] (per agevolare gli enti, in allegato alle Faq, è riportato uno schema di atto di designazione).
Indipendentemente dalla natura e dalla forma dell'atto utilizzato, è necessario che nello stesso sia individuato in maniera inequivocabile il soggetto che opererà come RPD, riportandone espressamente le generalità[11], i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del RGPD[12]) e le funzioni che questi sarà chiamato a svolgere in ausilio al titolare/responsabile del trattamento, in conformità a quanto previsto dal quadro normativo di riferimento.

[9] Sul tema della certificazione inoltre si richiama l'attenzione sul comunicato congiunto, pubblicato sul sito dell'Autorità il 18 luglio 2017 (doc. web n. 6621723), con il quale il Garante e ACCREDIA (l'Ente unico nazionale di accreditamento designato dal Governo italiano) hanno ritenuto necessario sottolineare - al fine di indirizzare correttamente le attività svolte dai soggetti a vario titolo interessati in questo ambito - che «al momento le certificazioni di persone, nonché quelle emesse in materia di privacy o data protection eventualmente rilasciate in Italia, sebbene possano costituire una garanzia e atto di diligenza verso le parti interessate dell'adozione volontaria di un sistema di analisi e controllo dei principi e delle norme di riferimento, a legislazione vigente non possono definirsi "conformi agli artt. 42 e 43 del regolamento 2016/679", poiché devono ancora essere determinati i "requisiti aggiuntivi" ai fini dell'accreditamento degli organismi di certificazione e i criteri specifici di certificazione».
[10] Al riguardo, si ricorda che la funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna al titolare/responsabile del trattamento. In tal caso, come indicato nelle citate Linee guida, è indispensabile che ciascun soggetto appartenente alla persona giuridica operante quale RPD soddisfi tutti i requisiti richiesti dal RGPD. Cfr. sul punto le indicazioni del Gruppo Art. 29 riportate nel paragrafo 2.5., pag. 12, e nella domanda n. 7, pag. 24, delle Linee guida.
[11] Secondo quanto precisato nelle Linee guida, se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In particolare, «per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi» (cfr. par. 2.5., pag. 12).
[12] Cfr. la Faq n. 7 in relazione alla preliminare valutazione sulla compatibilità di ulteriori compiti e funzioni da assegnare al RPD.

L'eventuale assegnazione di compiti aggiuntivi, rispetto a quelli originariamente previsti nell'atto di designazione, dovrà comportare la modifica e/o l'integrazione dello stesso o delle clausole contrattuali.
Nell'atto di designazione o nel contratto di servizi devono risultare succintamente indicate anche le motivazioni che hanno indotto l'ente a individuare, nella persona fisica selezionata, il proprio RPD, al fine di consentire la verifica del rispetto dei requisiti previsti dall'art. 37, par. 5 del RGPD, anche mediante rinvio agli esiti delle procedure di selezione interna o esterna effettuata. La specificazione dei criteri utilizzati nella valutazione compiuta dall'ente nella scelta di tale figura, oltre a essere indice di trasparenza e di buon amministrazione, costituisce anche elemento di valutazione del rispetto del principio di «responsabilizzazione».
Una volta individuato, il titolare o il responsabile del trattamento è tenuto a indicare, nell'informativa fornita agli interessati, i dati di contatto del RPD pubblicando gli stessi anche sui siti web e a comunicarli al Garante (art. 37, par. 7). Per quanto attiene al sito web, può risultare opportuno inserire i riferimenti del RPD nella sezione "amministrazione trasparente", oltre che nella sezione "privacy" eventualmente già presente.
Come chiarito nelle Linee guida, in base all'art. 37, par. 7, non è necessario -anche se potrebbe costituire una buona prassi, in ambito pubblico- pubblicare anche il nominativo del RPD, mentre occorre che sia comunicato al Garante per agevolare i contatti con l'Autorità (anche in questo caso, in allegato alle Faq, è riportato un modello di comunicazione al Garante). Resta invece fermo l'obbligo di comunicare il nominativo agli interessati in caso di violazione dei dati personali (art. 33, par. 3, lett. b)[13].

5. La designazione di un RPD interno all'autorità pubblica o all'organismo pubblico richiede necessariamente anche la costituzione di un apposito ufficio?

Il RGPD prevede, all'art. 38, par. 2, che «il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica».
Ne discende che, in relazione alla complessità (amministrativa e tecnologica) dei trattamenti e dell'organizzazione, occorrerà valutare attentamente se una sola persona possa essere sufficiente a svolgere il complesso dei compiti affidati al RPD. Come riportato anche nelle Linee guida, «in linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto»[14].
All'esito di questa analisi si potrà valutare quindi l'opportunità/necessità di istituire un apposito ufficio al quale destinare le risorse necessarie allo svolgimento dei compiti stabiliti. Ad ogni modo, ove sia costituito un apposito ufficio, è comunque necessario che venga sempre individuata la persona fisica che riveste il ruolo di RPD (mediante l'atto di designazione di cui sopra)[15].

---

[13] Cfr. al riguardo il paragrafo 2.6. delle Linee guida.
[14] Vedi sul punto Linee guida, paragrafo 3.2., pag. 15.
[15] Cfr., in proposito, la nota n. 4.

6. È ammissibile che uno stesso titolare/responsabile del trattamento abbia più di un RPD?

Alcune organizzazioni complesse hanno richiesto all'Autorità di valutare la possibilità di designare più RPD.

Al riguardo, si rileva che l'unicità della figura del RPD è una condizione necessaria per evitare il rischio di sovrapposizioni o incertezze sulle responsabilità, sia con riferimento all'ambito interno all'ente, sia con riferimento a quello esterno, e pertanto occorre che questa sia sempre assicurata.

Nulla osta, invece, all'individuazione di più figure di supporto, con riferimento a settori o ambiti territoriali diversi, anche dislocate presso diverse articolazioni organizzative dell'amministrazione, che facciano però riferimento a un unico soggetto responsabile, sia che la scelta ricada su un RPD interno, sia che questa ricada su un RPD esterno.

Infatti, in relazione alla particolare eterogeneità dei trattamenti di dati personali effettuati (in rapporto, ad esempio, all'effettuazione di trattamenti soggetti a basi giuridiche diverse in ambito di prevenzione, indagine, accertamento e perseguimento di reati) ovvero della complessità della struttura organizzativa dell'ente (talvolta molto ramificata a livello territoriale) può risultare opportuno individuare specifici "referenti" del RPD che potrebbero svolgere un ruolo di supporto e raccordo, sulla base di precise istruzioni del RPD, anche, se del caso, operando quali componenti del suo gruppo di lavoro[16].

7. Quali sono gli ulteriori compiti e funzioni che possono essere assegnati a un RPD?

Il RGPD consente l'assegnazione al RPD di ulteriori compiti e funzioni, a condizione che non diano adito a un conflitto di interessi (art. 38, par. 6e che consentano al RPD di avere a disposizione il tempo sufficiente per l'espletamento dei compiti previsti dal RGPD (art. 38, par. 2).

A seconda della natura dei trattamenti e delle attività e dimensioni della struttura del titolare o del responsabile, le eventuali ulteriori incombenze attribuite al RPD non dovrebbero pertanto sottrarre allo stesso il tempo necessario per adempiere alle relative responsabilità.

In linea di principio, è quindi ragionevole che negli enti pubblici di grandi dimensioni, con trattamenti di dati personali di particolare complessità e sensibilità, non vengano assegnate al RPD ulteriori responsabilità (si pensi, ad esempio, alle amministrazioni centrali, alle agenzie, agli istituti previdenziali, nonché alle regioni e alle asl). In tale quadro, ad esempio, avuto riguardo, caso per caso, alla specifica struttura organizzativa, alla dimensione e alle attività del singolo titolare o responsabile, l'attribuzione delle funzioni di RPD al responsabile per la prevenzione della corruzione e per la trasparenza, considerata la molteplicità degli adempimenti che incombono su tale figura, potrebbe rischiare di creare un cumulo di impegni tali da incidere negativamente sull'effettività dello svolgimento dei compiti che il RGPD attribuisce al RPD.

Rispetto all'assenza di conflitto di interessi, occorre inoltre valutare se, come indicato nelle Linee guida, le eventuali ulteriori funzioni assegnate non comportino la definizione di finalità e modalità del trattamento dei dati. Ciò significa che, a grandi linee, in ambito pubblico, oltre ai ruoli manageriali di vertice, possono sussistere situazioni di conflitto di interesse rispetto a figure apicali dell'amministrazione investite di capacità decisionali in ordine alle finalità

[16] In caso di RDP esterno, cfr. le note 4 e 5.

e ai mezzi del trattamento di dati personali posto in essere dall'ente pubblico, ivi compreso, ad esempio, il responsabile dei Sistemi informativi (chiamato ad individuare le misure di sicurezza necessarie), ovvero quello dell'Ufficio di statistica (deputato a definire le caratteristiche e le metodologie del trattamento dei dati personali utilizzati a fini statistici).
Riguardo agli ulteriori compiti e funzioni in capo al RPD, particolare attenzione andrebbe infine prestata nei casi di unico RPD tra molteplici autorità pubbliche e organismi pubblici, nonché nei casi di RPD esterno, in quanto questi potrebbe svolgere ulteriori compiti che comportano situazioni di conflitto di interesse oppure non essere in grado di adempiere in modo efficiente alle sue funzioni. In questi casi, nell'atto di designazione o nel contratto di servizio il RPD dovrà fornire opportune garanzie per favorire efficienza e correttezza e prevenire conflitti di interesse.

IV. La Commissione Europea pubblica orientamenti sulle nuove norme in materia di protezione dei dati.

Con un comunicato stampa del 24 gennaio 2018 la Commissione Europea ha reso nota la pubblicazione di alcuni orientamenti volti a facilitare l'applicazione diretta nell'UE delle nuove norme in materia di protezione dei dati[17].
Il nuovo regolamento, infatti, prevedendo un'unica serie di norme direttamente applicabili in tutti gli Stati membri, necessita ancora di notevoli adeguamenti per determinati aspetti, come la modifica delle leggi esistenti da parte degli Stati membri o dell'istituzione del Comitato europeo per la protezione dei dati da parte delle autorità di protezione dei dati[18].
Gli orientamenti delineano gli elementi principali delle nuove norme in materia di protezione dei dati:

- un'unica serie di norme in tutto il continente, per garantire la certezza giuridica per le imprese e lo stesso livello di protezione dei dati in tutta l'UE per i cittadini;
- applicazione delle stesse norme a tutte le imprese che offrono servizi nell'UE, anche se aventi la propria sede al di fuori dell'UE;
- diritti nuovi e più forti per i cittadini: il diritto all'informazione, il diritto di accesso e il diritto all'oblio sono rafforzati. Il nuovo diritto alla portabilità dei dati consente ai cittadini di trasferire i propri dati da

[17] Ad esempio è stato introdotto un nuovo strumento online per aiutare i cittadini, le imprese (soprattutto le PMI) e le organizzazioni a conformarsi alle nuove norme in materia di protezione dei dati.
[18] Da quando è stato adottato il regolamento generale sulla protezione dei dati, nel maggio 2016, la Commissione si è sempre impegnata attivamente con tutti i soggetti interessati (governi, autorità nazionali, imprese) al fine di predisporre l'applicazione delle nuove norme. Tuttavia il lavoro preparatorio sta progredendo a ritmi diversi nei vari Stati membri; ad oggi, solo due hanno già adottato la normativa nazionale pertinente. Gli Stati membri quindi dovrebbero accelerare l'adozione della legislazione nazionale e fare in modo che queste misure siano conformi al regolamento. Essi dovrebbero anche dotare le autorità nazionali delle necessarie risorse finanziarie e umane al fine di garantirne l'indipendenza e l'efficienza.
Alla luce di quanto detto la Commissione intende destinare 1,7 milioni di euro al finanziamento delle autorità di protezione dei dati e alla formazione dei professionisti in materia di protezione dei dati e altri 2 milioni per sostenere le autorità nazionali nell'opera di sensibilizzazione rivolta alle imprese, in particolare alle PMI.

un'impresa all'altra. Ciò offrirà alle imprese nuove opportunità commerciali;

- maggiore protezione contro le violazioni dei dati: le imprese sono tenute a notificare entro 72 ore all'autorità di protezione dei dati le violazioni dei dati che mettono a rischio le persone;
- norme rigorose e multe dissuasive: tutte le autorità di protezione dei dati avranno il potere di infliggere multe fino a un massimo di 20 milioni di euro o, nel caso di un'impresa, fino al 4% del fatturato annuo a livello mondiale.

Infine, la Commissione ricorda come fino al 25 maggio continuerà a sostenere attivamente gli Stati membri, le autorità di protezione dei dati e le imprese per aiutarli a prepararsi all'attuazione della riforma e che a partire da maggio 2018, essa, monitorerà le modalità di applicazione delle nuove norme da parte degli Stati membri e prenderà gli eventuali provvedimenti necessari.

V. Le modifiche introdotte con la legge di Bilancio 2018.

Nonostante quanto stabilito dal regolamento comunitario e sebbene fosse già stata conferita delega al governo per interventi correttivi e integrativi ai fini della piena applicazione del Gdpr (*General data protection regulation*), il legislatore è intervenuto sul tema con la legge di Bilancio 2018 (in particolare nell'art. 1, commi 1020-1025, della legge del 27 dicembre 2017, n. 205) stabilendo che il titolare di dati personali, ove effettui un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati, deve darne tempestiva comunicazione[19] al Garante per la protezione dei dati personali affinché quest'ultimo effettui una breve istruttoria sul rischio di lesione dei diritti e della libertà dei soggetti interessati[20].

Viene introdotta quindi un'ulteriore ipotesi di bilanciamento di interessi: in cui l' interesse del titolare viene riconosciuto legittimo dall'ordinamento qualora esso non contrasti coi diritti e le libertà dell'interessato[21].

In presenza di tale interesse ritenuto legittimo (cioè conforme ai principi generali e perseguito con correttezza) e in assenza di possibili contrasti con interessi sovraordinati dell'interessato, il trattamento dei dati potrà avvenire senza bisogno che l'interessato vi acconsenta.

È evidente che la reale portata di questa importante condizione di legittimità dipende dalla scelta di chi sia il soggetto competente ad effettuare il giudizio di ponderazione. Il regolamento generale sulla protezione dei dati, di cui si attende la piena applicazione a partire dal 25 maggio e che sostituirà le norme con esso incompatibili del codice privacy, ha operato una fondamentale scelta di metodo

---

[19] Cfr. art. 1, comma 1022, della legge del 27 dicembre 2017, n. 205, prevede che "*il titolare dei dati invia al Garante un'informativa relativa all'oggetto, alle finalità e al contesto di trattamento, utilizzando il modello di cui al comma 1021, lettera c). Trascorsi quindici giorni lavorativi dall'invio dell'informativa, in assenza di risposta da parte del Garante, il titolare può procedere al trattamento*".

[20] Cfr. art. 1, comma 1023, della legge del 27 dicembre 2017, n. 205.

[21] L'uso dei dati personali da parte di terzi finora è stato disciplinato dal legislatore secondo un fondamentale criterio di bilanciamento degli interessi in gioco: se non sussistono motivazioni di ordine superiore, tale uso è soggetto al potere di controllo di colui al quale i dati stessi si riferiscono; questo potere viene esercitato acconsentendo o meno all'uso che viene fatto dei propri dati. Viceversa, se le finalità d'uso sono ritenute dal legislatore prevalenti (come l'uso per obbligo di legge o nel perseguimento di un interesse pubblico), il trattamento viene autorizzato dallo stesso legislatore in sostituzione del consenso dell'individuo.

basata sulla responsabilizzazione del titolare ("*accountability*") e sull'approccio fondato sul rischio: il titolare deve attenersi alle prescrizioni di legge effettuando adeguate valutazioni basate sul rischio. Seguendo questa impostazione generale, il Gdpr rimette in capo all'ente la valutazione della sussistenza di un interesse legittimo del titolare suscettibile di rendere superfluo il consenso dell'interessato; qualora la valutazione risultasse erronea il titolare sarà suscettibile di sanzione[22].

Avv. Cristina Biglia
Dott. Eugenio Mariani

[22] Cfr. Riccardo Imperiali e Rosario Imperiali, *Privacy con meno responsabilità*, in Quotidiano Enti Locali & Pa, del 23 gennaio 2018.