La valutazione di impatto sulla protezione dei dati

di Gianluca Satta (*)

L'articolo offre una breve panoramica dei principali aspetti legati alla valutazione di impatto sulla protezione dei dati personali, fra le principali e più significative novità previste dal Reg. UE 2016/679 nell'ambito del nuovo modello di approccio alla privacy basato sul risk assessment.

Inquadramento generale

La valutazione di impatto sulla protezione dei dati personali (nota anche con l'acronimo inglese "DPIA - *Data Protection Impact Assessment*") rappresenta una delle principali e più significative novità previste dal Reg. UE 2016/679 (Regolamento Generale in materia di Protezione dei Dati, di seguito anche "Regolamento" o "RGPD"). In particolare, il concetto di valutazione di impatto sulla protezione dei dati è introdotto dall'art. 35 del Regolamento e dall'art. 27 della Direttiva UE 2016/680 (1), due strumenti normativi che insieme costituiscono il c.d. pacchetto protezione dati.

In termini generali, come meglio si vedrà nel prosieguo, la valutazione di impatto è una misura di natura preventiva che si incardina all'interno del nuovo modello di approccio alla *privacy* basato sul *risk assessment* del titolare, richiedendo l'attivazione di un vero e proprio processo di valutazione del trattamento volto a definirne la necessità, la proporzionalità e la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, con l'obiettivo di individuare i suddetti rischi e le misure adeguate per mitigare e ridurre al minimo gli effetti pregiudizievoli.

Come si evince dal dato normativo, la valutazione di impatto non è richiesta per tutti i trattamenti effettuati dal titolare, bensì è necessaria soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (2). Il compito di effettuare la valutazione in merito alla presenza o meno del rischio elevato spetta, quindi, al titolare del trattamento; per queste ragioni, tale adempimento rientra nell'ambito delle c.d. misure di responsabilizzazione (3) (o *accountability* nell'accezione inglese) in quanto consente al titolare di rispettare i requisiti previsti in materia di protezione dei dati personali e, allo stesso tempo, di dimostrare l'adeguatezza delle misure adottate per garantire la conformità al Regolamento (4).

Inoltre, in linea con il principio di neutralità che caratterizza l'intero impianto normativo del Regolamento, anche in materia di valutazione di impatto le norme di riferimento non definiscono una particolare metodologia da seguire per effettuare l'analisi bensì, oltre ad individuare i casi in cui la valutazione si considera necessaria, si limitano esclusivamente ad inquadrare, in termini generali, tutti gli aspetti che devono essere presi in considerazione e i requisiti minimi sul contenuto della valutazione

Note:

(*) Avvocato in Cagliari, cultore in materia di Diritto dell'Informatica delle Nuove Tecnologie presso l'Università degli Studi di Cagliari

(1) Direttiva UE 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

(2) Art. 35, par. 1, RGPD.

(3) Le misure di responsabilizzazione costituiscono una grande novità per la protezione dei dati personali in quanto, contrariamente a quanto accadeva in passato, è affidato ai titolari del trattamento "il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali - nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel Regolamento.". Autorità Garante per la protezione dei dati personali, in www.garanteprivacy.it.

(4) In questo senso si esprime anche il considerando n. 84 del Regolamento: "L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente Regolamento.".

di impatto senza fornire, peraltro, alcuna definizione del termine (5). Prima di esaminare nello specifico gli aspetti peculiari della DPIA, è doveroso fare un breve accenno al rapporto di quest'ultima con alcuni istituti previsti dal Codice della *privacy* (6) al fine di meglio comprenderne la portata innovativa e individuare le differenze e gli elementi di continuità rispetto a quanto previsto dal Codice; in particolare, il riferimento è agli istituti della "richiesta di autorizzazione al Garante" e della "verifica preliminare". Il primo adempimento, richiesto obbligatoriamente per il trattamento di dati sensibili e genetici, è finalizzato ad ottenere l'autorizzazione dell'Autorità Garante per procedere al trattamento di tali dati (7). Il secondo, invece, consiste nell'intervento dell'Autorità Garante al fine di individuare misure ed accorgimenti per il trattamento di dati, diversi da quelli sensibili e giudiziari, che presenta rischi specifici per i diritti e le libertà fondamentali (8).

Gli elementi comuni dell'attuale disciplina, rispetto a quella prevista dal Codice, si concentrano esclusivamente sui presupposti che determinano la necessità di ricorrere a tali adempimenti. Infatti, sia la richiesta di autorizzazione che la verifica preliminare sono previsti ogni qual volta il trattamento riserva particolari rischi per i diritti e le libertà delle persone; nel primo caso il rischio è insito nella particolare natura dei dati coinvolti (dati sensibili e genetici) nel secondo, invece, il rischio è oggetto di valutazione specifica e coinvolge tutti i dati personali diversi da quelli sensibili e giudiziari. Allo stesso modo, come già evidenziato, anche la valutazione di impatto sulla protezione dei dati personali, prevista dal nuovo Regolamento, è richiesta ogni qual volta si presenta un rischio elevato per i diritti e le libertà delle persone fisiche.

L'aspetto di evidente discontinuità e di maggiore novità, invece, è rappresentato dal fatto che, mentre nel Codice della *privacy* la valutazione in merito ai rischi sui diritti e sulle libertà delle persone è effettuata dall'Autorità Garante all'interno dei propri provvedimenti, con la valutazione di impatto sulla protezione dei dati il giudizio sull'incidenza dei rischi è rimesso all'esclusiva valutazione del titolare del trattamento.

Infine, a conferma del particolare rapporto tra gli adempimenti previsti dal Codice della *privacy* e la valutazione di impatto sulla protezione dei dati, secondo quanto stabilito nelle Linee Guida in materia di valutazione di impatto (9), non si ritiene necessario procedere ad una valutazione d'impatto per i trattamenti che sono già stati oggetto di verifica da parte di un'autorità di controllo, a norma dell'art. 20 della Direttiva 95/46/CE (10), se eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente. In coerenza con quanto appena affermato, lo stesso legislatore europeo ha ritenuto opportuno evidenziare che "le autorizzazioni delle autorità di controllo basate sulla Direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate." (11).

> La valutazione di impatto sulla protezione dei dati personali è finalizzata ad attivare un vero e proprio processo di gestione dei rischi.

La valutazione di impatto nel Regolamento privacy

La valutazione di impatto sulla protezione dei dati personali è finalizzata ad attivare un vero e

Note:

(5) Il significato e il ruolo della valutazione di impatto sono meglio inquadrati nel considerando n. 84 del Regolamento: "Per potenziare il rispetto del presente Regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.".

(6) D.Lgs. 30 giugno 2003, n. 196.

(7) Cfr. art. 26, 90 e 107 del D.Lgs. 30 giugno 2003, n. 196. Per un maggiore approfondimento in merito alla richiesta di autorizzazione, si veda M. Farina - F. Voltan, *La nuova privacy*, 2011. L'Autore, in particolare, evidenzia come: "L'autorizzazione costituisce una condizione di liceità del trattamento dei dati sensibili (e talvolta dei dati giudiziari). Si tratta di un provvedimento del Garante mediante cui l'autorità, dopo aver esaminato che il trattamento in questione non comporta particolari rischi di danno o di pericolo per i diritti, le libertà fondamentali e la dignità delle persone lo acconsente" (pag. 41).

(8) Cfr. art. 17 del D.Lgs. 30 giugno 2003, n. 196.

(9) Gruppo di lavoro art. 29 in materia di protezione dei dati personali, "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento 'possa presentare un rischio elevato' ai fini del Regolamento (UE) 2016/679" adottate il 4 aprile 2017 - Versione emendata e adottata in data 4 ottobre 2017.

(10) L'art. 20 della Direttiva 95/46/CE disciplina il c.d. controllo preliminare, poi recepito nel nostro ordinamento con l'introduzione dell'istituto della verifica preliminare.

(11) Cfr. Considerando n. 171 RGPD.

proprio processo di gestione dei rischi e deve essere inquadrata nell'ambito del più generale obbligo, a cui sono soggetti i titolari del trattamento, di adottare misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare il rispetto e la conformità al Regolamento, tenuto conto "dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (12).
Il concetto di "rischio", che qui rileva, si riferisce a tutti gli eventi e le conseguenze pregiudizievoli da essi derivanti, misurati in termini di gravità e probabilità, che il titolare deve gestire mediante l'adozione di una serie di procedure, attività e soluzioni (tecniche e organizzative) in grado di permetterne l'individuazione, l'analisi, la stima, la valutazione, la mitigazione e la rivalutazione. Il riferimento ai "diritti e le libertà delle persone fisiche", invece, deve estendersi fino a comprendere tutti i diritti alla protezione dei dati e alla vita privata, nonché gli altri diritti fondamentali quali la libertà di espressione, di pensiero, di coscienza, di religione, di circolazione e il divieto di discriminazione.
Secondo l'art. 35 del Regolamento, quindi, la valutazione di impatto sulla protezione dei dati personali è necessaria ogni qual volta il titolare rilevi che il trattamento, considerata la natura, l'oggetto, il contesto e le finalità del trattamento, possa "presentare un rischio elevato per i diritti e le libertà delle persone fisiche". In particolare, la valutazione di impatto assume particolare importanza quando viene introdotta una nuova tecnologia in relazione al trattamento dei dati personali (13).
Pur trattandosi di un'elencazione meramente esemplificativa e non esaustiva, l'art. 35, paragrafo 3, fornisce alcuni esempi nei quali la presenza di rischi elevati è intrinseca nella natura dell'attività sottesa al trattamento; in particolare, il riferimento è ai 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'art. 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'art. 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".
Dall'analisi dei suddetti casi emerge, quindi, che la valutazione di impatto sia necessaria quando il trattamento è finalizzato alla valutazione o all'assegnazione di un punteggio, compresa la profilazione, in particolare quando riguarda "il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (14). Allo stesso modo, il rischio si considera elevato quando il titolare effettua un trattamento di dati finalizzato a consentire l'adozione di decisioni in merito agli interessati da cui possano derivare particolari effetti giuridici o che incidono in modo analogo significativamente sulle persone, mediante un processo decisionale automatizzato.
Allo stesso modo, i rischi si considerano elevati quando il trattamento è effettuato su larga scala e riguarda dati di natura particolarmente sensibile e personale, come quelli previsti dall'art. 9 e dall'art. 10 del Regolamento (15). L'assenza di un riferimento normativo e di parametri valutativi precisi, non consente di definire con precisione la quantità di dati oggetto di trattamento o il numero di interessati ricompresi nel concetto di "larga scala". Tuttavia, al fine di stabilire se un trattamento sia o meno su larga scala, i fattori più rilevanti sono: il numero o la percentuale di soggetti interessati dal trattamento, il volume e/o le diverse tipologie di dati oggetto di trattamento, la durata e la portata geografica del trattamento (16).

Note:
(12) Cfr. art. 24, par. 1, RGPD.
(13) Tale considerazione emerge, in particolare, dal dato letterale presente nell'inciso dell'art. 35 del Regolamento "allorché prevede in particolare l'uso di nuove tecnologie" e dai considerando n. 89 e 91 del Regolamento.
(14) Cfr. considerando n. 71 e 91 RGPD.
(15) Il riferimento è ai dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 RGPD) e ai dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 RGPD).
(16) Un ulteriore criterio interpretativo è fornito dallo stesso legislatore, nel considerando n. 91 del Regolamento, secondo cui un trattamento avviene su larga scala quando ha ad oggetto "una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati".

Infine, in relazione all'ultimo dei casi, anche il trattamento di dati effettuato tramite il monitoraggio sistematico degli interessati o la sorveglianza su larga scala di una zona accessibile al pubblico implica la presenza di elevati rischi; tale considerazione deriva dal fatto che, per le caratteristiche e le modalità di raccolta dei dati, gli interessati potrebbero non essere pienamente consapevoli dell'attività di trattamento o non essere in grado di sottrarsi a tale trattamento, in particolare quando questo avviene nel contesto di spazi pubblici (o ad accesso pubblico).

La natura preventiva della valutazione di impatto impone che tale adempimento sia posto in essere prima che abbiano inizio le operazioni di trattamento e, se possibile, sin dalla fase di progettazione del trattamento.

Le Linee Guida in materia di valutazione di impatto individuano anche ulteriori criteri utili per l'individuazione dei trattamenti che richiedono una valutazione di impatto in virtù del rischio elevato intrinseco. In particolare, si tratta dei casi in cui il trattamento: comporta la creazione di corrispondenze o la combinazione di insiemi di dati (17); riguarda dati relativi ad interessati particolarmente vulnerabili (18); prevede la combinazione di diverse soluzioni e applicazioni tecnologiche ed organizzative (19); e, infine, impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (20).

La presenza di una o più condizioni, tra quelle sin qui esaminate, quindi, comporta l'obbligo per il titolare del trattamento di effettuare la valutazione di impatto sulla protezione dei dati. In ogni caso, in virtù del principio di responsabilizzazione, il titolare del trattamento è sempre tenuto a documentare e giustificare le ragioni che lo hanno indotto a non effettuare la valutazione di impatto, sia nel caso in cui le suddette condizioni non sussistono, sia quando, pur in presenza delle stesse, il trattamento è stato valutato privo di rischi elevati. Peraltro, è doveroso evidenziare come l'onere di motivare e documentare la propria scelta sussiste anche negli altri casi in cui la valutazione di impatto non è considerata obbligatoria, e precisamente:

- quando è stata già effettuata la DPIA per un trattamento simile e che presenta rischi analoghi (art. 35, paragrafo 1). In questi casi è possibile utilizzare i risultati della valutazione di impatto già effettuata a condizione che i trattamenti siano molto simili per natura, ambito di applicazione, contesto e finalità;
- qualora il trattamento sia già stato oggetto di verifica ai sensi dell'art. 20 della Direttiva 95/46/CE da parte di un'autorità di controllo e non presenta alcuna variazione;
- qualora un trattamento, effettuato a norma dell'art. 6, paragrafo 1, lett. c) o e), trovi la sua base giuridica nel diritto dell'Unione o nel diritto dello Stato membro e tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica, salvo che lo Stato membro non abbia previsto la necessità di effettuare tale valutazione prima di procedere alle attività di trattamento (art. 35, paragrafo 10);
- quando il trattamento in questione è incluso nell'elenco delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati, pubblicato dall'autorità di controllo (art. 35, paragrafo 5) (21).

La presenza di una delle condizioni di esclusione della valutazione di impatto, tuttavia, non elimina l'obbligo generale per il titolare del trattamento di attuare ogni misura volta a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In questo senso, quindi, considerata la rapida evoluzione nel

Note:

(17) Simili attività potrebbero implicare un trattamento svolto per finalità diverse da quelle originariamente dichiarate all'interessato ovvero da un titolare diverso da quello iniziale, in contrasto con le ragionevoli aspettative dell'interessato.

(18) Il riferimento è ai soggetti minori o altri interessati nell'ambito di un rapporto (anche contrattuale) che presenta degli squilibri di potere tali da impedire all'interessato di esprimere un effettivo controllo sull'attività di trattamento.

(19) L'uso di nuove tecnologie, oltre ad accrescere notevolmente la capacità di effettuare operazioni di trattamento complesse, potrebbe comportare conseguenze sul piano personale e sociale sconosciute agli utilizzatori.

(20) In questo senso, si veda l'art. 22 e il considerando n. 91 RGPD.

(21) L'elenco potrà prevedere l'esclusione della valutazione di impatto per tutti i trattamenti che siano conformi alle condizioni specifiche dettate dall'autorità di controllo attraverso linee guida, decisioni o autorizzazioni specifiche. In particolare, in tali casi è richiesto che l'autorità di controllo competente proceda nuovamente alla valutazione per verificarne l'attualità e la conformità al Regolamento, e l'esclusione sarà consentita solo se il trattamento rientri a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco.

tempo delle operazioni di trattamento e delle vulnerabilità connesse, la valutazione di impatto sulla protezione dei dati deve essere inquadrata come un'attività strategicamente mirata a favorire il continuo monitoraggio dei processi e il miglioramento del livello di protezione dei dati in un contesto di continuo mutamento.

Ciascun titolare del trattamento potrà modulare e variare la propria valutazione di impatto sulla base della complessità dei processi e dei trattamenti in questione.

Indicazioni operative sulla valutazione di impatto

La natura preventiva della valutazione di impatto sulla protezione dei dati impone necessariamente che tale adempimento sia posto in essere prima che abbiano inizio le operazioni di trattamento e, per quanto possibile, sin dalla fase di progettazione del trattamento, in ossequio al principio della "*data protection by design and by default*". Non vi è dubbio, infatti, che l'esecuzione della valutazione di impatto agevola notevolmente il rispetto di quanto previsto dall'art. 25 del Regolamento, secondo cui il titolare del trattamento è tenuto ad adottare "misure tecniche e organizzative adeguate" al fine di dare attuazione ai principi di protezione dei dati e ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati tenendo conto, fra le altre, dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento".

Il compito di effettuare la DPIA spetta, in via principale, al titolare del trattamento (22) il quale, per l'esecuzione materiale dell'attività, può rivolgersi ad un soggetto interno o esterno all'organizzazione, pur mantenendo sempre la responsabilità generale dell'adempimento. Inoltre, il titolare deve sempre consultarsi con il responsabile della protezione dei dati (in inglese *Data Protection Officer*), qualora sia stato designato, e il parere fornito dovrà essere documentato all'interno della valutazione di impatto.

Nell'ambito delle attività inerenti l'esecuzione della valutazione di impatto, se necessario, il titolare può raccogliere anche le opinioni degli interessati o dei loro rappresentanti sul trattamento oggetto della valutazione, al fine di poter assumere decisioni più aderenti alle esigenze del caso concreto (23); in ogni caso, il titolare del trattamento dovrà sempre giustificare la propria scelta quando non provvede a coinvolgere gli interessati e dovrà sempre documentare ogni decisione in merito, anche qualora intenda disattendere le opinioni fornite dagli interessati.

Per quanto concerne il profilo operativo, il Regolamento non individua delle particolari metodologie da seguire, ma si limita a definire alcuni criteri comuni in merito ai contenuti e alle caratteristiche minime della valutazione di impatto; in questo modo, ciascun titolare del trattamento potrà modulare e variare la propria valutazione di impatto sulla base della complessità dei processi e dei trattamenti in questione. In particolare, secondo l'art. 35, paragrafo 7, del Regolamento, il documento contenente la valutazione di impatto deve includere almeno: la descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, la valutazione dei rischi per i diritti e le libertà degli interessati e, infine, deve elencare tutte le misure previste per affrontare i rischi individuati, 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 in questione (24).

Note:

(22) Quando il trattamento è eseguito, integralmente o parzialmente, da un responsabile del trattamento, quest'ultimo ha il dovere di assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati e fornire tutte le informazioni necessarie, in conformità all'art. 28, par. 3, lett. f).

(23) Le modalità di raccolta delle opinioni sono liberamente determinate dal titolare del trattamento, purché la stessa attività sia eseguita nel rispetto delle regole generali sul trattamento dei dati personali.

(24) La valutazione di impatto sulla protezione dei dati ha ad oggetto la gestione del rischio per i diritti e le libertà delle persone fisiche e pertanto, per una corretta analisi, è necessario adottare il punto di vista e la prospettiva degli interessati. Sotto questo profilo, quindi, la valutazione dei rischi nell'ambito della DPIA non coincide con la valutazione dei rischi nell'ambito delle misure di sicurezza, ove l'oggetto è rappresentato dalla gestione dei rischi sui dati personali (e non sulle persone fisiche).

La DPIA deve concludersi con la redazione di un documento che dovrà essere conservato ed esibito all'autorità in caso di richiesta e, a discrezione del titolare del trattamento, potrà essere pubblicato (anche in forma sintetica) al fine di favorire una maggiore fiducia e trasparenza, in particolar modo se la valutazione di impatto è stata elaborata a seguito della consultazione degli interessati.

La DPIA deve concludersi con la redazione di un documento che dovrà essere conservato ed esibito all'autorità in caso di richiesta e, a discrezione del titolare del trattamento, potrà essere pubblicato.

Al termine della valutazione di impatto, qualora non sia possibile individuare misure adeguate a mitigare e ridurre i rischi sui diritti e sulle libertà delle persone a un livello accettabile, ovvero i rischi residui permangono in misura elevata, il titolare del trattamento dovrà obbligatoriamente rivolgersi all'autorità di controllo secondo il meccanismo della consultazione preventiva, previsto dall'art. 36 del Regolamento.
Infine, per quanto concerne il profilo sanzionatorio, in caso di violazione delle norme previste in materia di valutazione di impatto, oltre all'esercizio dei poteri correttivi previsti dall'art. 53 del Regolamento, l'autorità di controllo può infliggere anche le sanzioni pecuniarie secondo i criteri e i valori di cui all'art. 83, paragrafo 4, del Regolamento. Nello specifico, la mancata esecuzione della valutazione di impatto nei casi in cui è richiesta (25), ovvero l'errata esecuzione della valutazione (26) e la mancata consultazione dell'autorità di controllo quando è richiesto (27), possono comportare l'applicazione di una sanzione amministrativa pecuniaria fino a dieci milioni di euro o, nel caso di un'impresa, fino due punti percentuale del fatturato annuo globale dell'anno precedente.

Note:
(25) Cfr. art. 35, par. 1, 3 e 4, RGPD.
(26) Cfr. art. 35, par. 2, 7, 8 e 9, RGPD.
(27) Cfr. art. 36, par. 3, lett. e), RGPD.