GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERA 11 ottobre 2018, n. 467

G.U.R.I. 19 novembre 2018, n. 269

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati, ai sensi dell'articolo 35, comma 4, del regolamento (UE) n. 2016/679. (Delibera n. 467).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, di seguito «RGPD»);

Visto, in specie, l'art. 35, paragrafo 1, del RGPD, che stabilisce l'obbligo per il titolare di effettuare, prima dell'inizio del trattamento, una valutazione dell'impatto del trattamento medesimo, laddove quest'ultimo possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, «allorchè preved[a] in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità [...]»;

Visto il paragrafo 3 del medesimo articolo, che individua alcune ipotesi in cui è richiesta la valutazione d'impatto;

Visto il paragrafo 10 del predetto art. 35, che individua invece le ipotesi in cui tale valutazione non è richiesta, in particolare «qualora il trattamento effettuato ai sensi dell'art. 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica [...], salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento»;

Considerato che l'art. 35, paragrafo 4, rimette alle autorità di controllo nazionali il compito di redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto e di comunicarlo al Comitato europeo per la protezione dei dati di cui all'art. 68 del RGPD;

Considerato che il paragrafo 6 del citato art. 35 stabilisce l'applicazione del meccanismo di coerenza di cui all'art. 63 del RGPD, da parte della singola autorità di controllo competente, qualora l'elenco comprenda «attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione»;

Viste le indicazioni contenute nei «considerando» numeri 71, 75 e 91 del RGPD;

Viste le «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) n. 2016/679» del Gruppo di lavoro art. 29 per la protezione dei dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (di seguito «WP 248, rev. 01»), che hanno individuato i seguenti nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un «rischio elevato»: 1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di «aspetti riguardanti 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»; 2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3) monitoraggio sistematico degli interessati; 4) dati sensibili o dati aventi carattere altamente personale; 5) trattamento di dati su larga scala; 6) creazione di corrispondenze o combinazione di insiemi di dati; 7) dati relativi a interessati vulnerabili; 8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; 9) quando il trattamento in sè «impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto»);

Rilevato che il ricorrere di due o più dei predetti criteri è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e per il quale è quindi richiesta una valutazione d'impatto sulla protezione dei dati (cfr. WP 248, rev. 01, pag. 11);

Considerato che il garante ha predisposto un elenco delle tipologie di trattamento ai sensi dell'art. 35, paragrafo 4 da sottoporre a valutazione d'impatto;

Considerato che le previsioni di cui all'art. 35, paragrafo 1 del RGPD, che dispongono che «quando un tipo di trattamento, allorchè prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali», prevalgono in ogni caso;

Considerato altresì che il predetto elenco è stato predisposto sulla base del WP 248, rev. 01, allo scopo di specificarne ulteriormente il contenuto e a complemento dello stesso;

Rilevato che tale elenco è stato comunicato in data 11 luglio 2018 al Comitato per il prescritto parere (art. 35, paragrafi 4 e 6, e dall'art. 64, paragrafo 1, lettera a), del RGPD);

Viste le osservazioni rese dal Comitato nel parere adottato il 25 settembre 2018 e notificato il 2 ottobre 2018 (disponibile su https://edpb.europa.eu);

Ritenuto, in ottemperanza a quanto previsto dall'art. 64, paragrafo 7, del RGPD, di aderire alle osservazioni contenute nel suddetto parere e di modificare, in conformità, il relativo progetto di decisione e di darne comunicazione al presidente del Comitato;

Rilevato che tale elenco è riferito esclusivamente a tipologie di trattamento soggette al meccanismo di coerenza e che non è esaustivo, restando fermo quindi l'obbligo di adottare una valutazione d'impatto sulla protezione dei dati laddove ricorrano due o più dei criteri individuati dal WP 248, rev. 01 e che in taluni casi «un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno [dei predetti] criteri richieda una valutazione d'impatto sulla protezione dei dati» (cfr. WP 248, rev. 01, pag. 11);

Rilevato, altresì, che il predetto elenco potrà essere ulteriormente modificato o integrato anche sulla base delle risultanze emerse nel corso della prima fase di applicazione del RGPD;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del garante n. 1/2000;

Relatore il dott. Antonello Soro;

Tutto ciò premesso:

a) ai sensi degli articoli 35, paragrafo 4, e 57, paragrafo 1, lettera k), del RGPD fermo restando quanto indicato nel richiamato WP 248, rev. 01, individua l'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, riportate nell'allegato 1 facente parte integrante del presente provvedimento, che specificano quanto riportato nel citato WP 248, rev. 01;

b) ai sensi dell'art. 64, paragrafo 7 del RGPD comunica al presidente del Comitato il presente provvedimento che recepisce i rilievi formulati nel parere richiamato in premessa;

c) invia copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 11 ottobre 2018

Il presidente e relatore: SORO

Il segretario generale: BUSIA

ALLEGATO 1

1. Trattamenti valutativi o di scoring su larga scala, nonchè trattamenti che comportano la profilazione degli interessati nonchè lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad «aspetti riguardanti 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».

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono «effetti giuridici» oppure che incidono «in modo analogo significativamente» sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonchè il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri numeri 3, 7 e 8).

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.