DOSSIER
Regolamento UE Privacy: novità e adempimenti in vista della scadenza del 25 maggio

Introduzione

di **Teresa Cianni**
Settore Fse - Tecnostruttura

Il prossimo 25 maggio diventerà definitivamente applicabile in via diretta in tutti i Paesi UE il nuovo Regolamento europeo in materia di protezione dei dati personali (Reg. (UE) 2016/679).

Il Regolamento (in inglese GDPR) è stato pubblicato sulla Gazzetta ufficiale della UE (GUUE) il 4 maggio 2016, prevedendo un lasso temporale di due anni per il perfetto allineamento, da parte degli Stati membri, fra la normativa nazionale e le sue disposizioni. Unitamente alla Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini, costituisce il nuovo "Pacchetto protezione dati", l'insieme normativo che definisce un quadro comune in materia di tutela dei dati personali per tutti gli Stati membri della UE. L'obiettivo è quello di assicurare un'applicazione coerente ed omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche, con riguardo alla tutela dei dati personali, in tutta l'Unione, in modo da facilitare la libera circolazione dei dati personali nel mercato interno, segnando così il passaggio da un diritto alla protezione dei dati di tipo nazionale/individuale ad un diritto di tipo europeo/sociale.

Cionondimeno lo stesso Regolamento prevede uno spazio di manovra degli Stati membri per precisarne le norme, anche con riguardo a particolari categorie di dati (dati sensibili). In tal senso non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggior precisione i vincoli in base ai quali il trattamento di dati personali è lecito (cfr. C*onsiderando* 10). In proposito si rileva come a livello di ordinamento interno, lo scorso 6 novembre, sia stata pubblicata nella Gazzetta ufficiale della Repubblica Italiana una Legge delega al governo (L. 163/2017 art. 13) per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679. Tale allineamento dovrà avvenire entro sei mesi dalla data di entrata in vigore della legge delega, quindi entro il 21 maggio 2018.

Nel confermare che il trattamento dei dati deve basarsi sul consenso dell'interessato e avvenire in conformità ai principi di liceità, correttezza, trasparenza e proporzionalità, il Regolamento introduce una serie di innovazioni dirette a rafforzare i diritti fondamentali degli individui (diritto di accesso, di rettifica, diritto alla cancellazione/oblio, diritto di limitare il

trattamento, diritto alla portabilità dei dati e di opposizione al trattamento). Accresce, inoltre, le responsabilità del titolare e del responsabile del trattamento con la positivizzazione del principio di *accountability*, che sostituisce il principio autorizzativo attualmente vigente, con la finalità di porre chi tratta i dati personali in una posizione di ridurre i rischi di operazioni non conformi o non consentite motivando, in tal senso, il titolare e il responsabile a comportamenti e prassi virtuose.

Nelle more della modifica della legislazione nazionale, nei paragrafi che seguono si propone una disamina dei principali fattori di novità introdotti dal Regolamento UE rispetto alla disciplina attualmente vigente (D.lgs. 196/2003), mettendo in evidenza gli aspetti di maggior rilievo per le Regioni e rinviando per gli opportuni approfondimenti all'analisi della normativa e alle Linee guida elaborate dal Garante per la privacy **(1)**.

A corredo si forniscono alcune prime indicazioni alle amministrazioni sia in qualità di titolari sia nel ruolo di responsabili del trattamento in merito agli adempimenti da porre in essere per adeguarsi al rinnovato quadro legislativo. Nello specifico si distinguono i nuovi adempimenti, mettendoli in relazione ai soggetti del trattamento (titolare e responsabile), da quelli che discendono da modifiche a disposizioni già presenti nella disciplina nazionale. Considerata la particolare attenzione che in ambito FSE è da molto tempo prestata al tema della tutela dei dati, si riportano inoltre alcune indicazioni di massima per le AdG in merito ai risvolti per i trattamenti effettuati in tale settore e alle possibili iniziative da mettere in campo.

Note:

(1): Cfr. Guida all'applicazione del Regolamento UE 2016/679.

DOSSIER
Novità introdotte dal Regolamento

Novità introdotte dal Regolamento

Con riferimento ai diritti degli interessati, il Regolamento rafforza innanzitutto la disciplina del consenso introducendo una vera e propria definizione **(2)** ed alcuni elementi di attenzione per quanto concerne i dati sensibili e il consenso dei minori.

In linea generale il consenso deve essere: libero, specifico, informato e inequivocabile; non è ammesso il consenso tacito o presunto. Esso non deve essere reso necessariamente in forma scritta e può essere manifestato attraverso dichiarazione o azione positiva inequivocabile e concludente (es. la selezione di un'apposita casella di un sito web o una dichiarazione o qualsiasi altro comportamento che indichi chiaramente la volontà dell'interessato di accettare il trattamento proposto).

Per i dati "sensibili" il consenso deve essere "esplicito" (art. 9). Esso non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito". Il titolare, inoltre, deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento (art. 7, c. 1).

Il consenso dei minori è valido a partire dai 16 anni; prima di tale età il consenso deve essere prestato dal titolare della responsabilità genitoriale o da chi ne fa le veci (art. 8, c. 1).

Vengono ampliati (rispetto al Codice nazionale) i contenuti dell'informativa che deve essere fornita all'interessato, da parte del titolare o del responsabile del trattamento, a tutela dell'esercizio della protezione dei dati. I contenuti dell'informativa sono elencati in modo tassativo all'articolo 13 del Regolamento. In aggiunta agli elementi previsti dall'art. 13 del D.lgs. 196/2003, dovranno essere specificati: i dati di contatto del responsabile della protezione dei dati (RDP), la base giuridica del trattamento, il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, il diritto dell'interessato di ottenere la limitazione del trattamento, la portabilità dei dati e di presentare un reclamo all'autorità di controllo.

Il Regolamento specifica, inoltre, con un maggior grado di dettaglio rispetto al Codice in

vigore, le caratteristiche dell'informativa, che deve essere concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; si sottolinea inoltre la necessità di utilizzare un linguaggio chiaro e semplice, in particolare quando le informazioni sono destinate ai minori. L'informativa è fornita, in linea di principio, per iscritto e, se del caso, in formato elettronico (cfr. art. 12 e *Considerando* 58).

Viene ampliata la tutela degli interessati mediante l'introduzione del diritto alla cancellazione dei dati (diritto all'oblio) nei casi in cui: i dati personali non siano più necessari rispetto alle finalità per le quali sono stati raccolti e trattati, sia stato revocato il consenso o l'interessato si sia opposto al trattamento (art. 17).

Si prevede ancora la possibilità di ottenere, dal titolare, una limitazione del trattamento nelle ipotesi in cui l'interessato contesti l'esattezza dei dati o si sia opposto al trattamento (art. 18). Si tratta di un diritto diverso e più esteso rispetto al blocco del trattamento già previsto dal Codice, esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento e quale alternativa alla cancellazione dei dati, bensì anche nelle more che sia riscontrata da parte del titolare una richiesta di rettifica dei dati o di opposizione al trattamento.

Alla stessa stregua viene conferito all'interessato il diritto alla portabilità dei dati, ossia il diritto di ricevere i propri dati personali in un formato strutturato, di uso comune e leggibile da dispositivo automatico, qualora il trattamento si basi sul consenso e sia effettuato con mezzi automatizzati. Se tecnicamente fattibile, lo stesso ha (altresì) il diritto di ottenere la trasmissione diretta dei dati da un titolare ad un altro (art. 20).

Viene poi fissato un termine certo per la risposta all'interessato, in caso di esercizio del diritto di accesso o degli altri diritti di cui agli artt. da 16 a 22. In particolare il titolare del trattamento deve fornire le informazioni relative all'azione intrapresa entro 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il riscontro all'interessato deve essere comunque dato entro 1 mese dalla richiesta, anche in caso di diniego (art. 12, c. 3).

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, c. 1; art. 15, c. 3).

Con riferimento alle figure coinvolte nel trattamento dei dati (titolare, responsabile, incaricato) il Regolamento disciplina la contitolarità del trattamento (art. 26) 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.

Fissa, poi, più dettagliatamente (rispetto all'art. 29 del Codice) 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) che vincoli il responsabile al titolare del trattamento e che stipuli 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 (art. 28).

Consente la nomina di sub-responsabili del trattamento da parte di un responsabile (art. 28, c. 4) per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde nei confronti del titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di potenziali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (art. 82, commi 1 e 3).

Prevede obblighi specifici in capo ai responsabili del trattamento, distinti da quelli che pertengono ai titolari, con particolare riguardo alla tenuta del registro dei trattamenti svolti; l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti; la designazione di un responsabile della protezione dei dati.

Pur non prevedendo espressamente la figura dell'"incaricato" del trattamento (ex art. 30 del Codice), il Regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (art. 4, c. 10).

Il Regolamento pone con forza l'accento sulla "*accountability*" del titolare e del responsabile del trattamento, conferendo loro una maggiore responsabilità che si configura come una sostanziale assunzione di rischio nell'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione delle sue prescrizioni. Viene, in sostanza, affidato ai titolari 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 (art. 24).

Il primo di questi riguarda l'introduzione delle misure di sicurezza e delle misure di tutela e garanzia dell'interessato nel trattamento dei suoi dati fin dalla progettazione degli strumenti utilizzati (*privacy by design,* art. 25, c. 1 e *Considerando* 78). Le misure strumentali allo scopo sono: la migliore applicazione del principio di minimizzazione dei dati personali oggetto del trattamento, tanto con riferimento alla quantità dei dati, tanto ai tempi di conservazione e ai livelli di accessibilità, tanto alle prefissate finalità; la pseudonimizzazione ovvero l'oscuramento (reversibile) dei dati identificativi del soggetto interessato; la definizione di dati personali e tempi strettamente necessari al trattamento, in relazione alle diverse finalità.

Il secondo criterio riguarda l'analisi del rischio inerente il trattamento. Allo scopo si introducono la metodologia della valutazione preventiva d'impatto e la gestione del rischio e delle correlate misure di sicurezza.

Il titolare del trattamento dovrà effettuare una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali, quando il trattamento prevede l'utilizzo di nuove tecnologie e (considerati la natura, l'oggetto e la finalità) può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione può esaminare un insieme di trattamenti simili, che presentano rischi elevati analoghi, ed è richiesta nei casi di: 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; trattamento, su larga scala **(3)**, di categorie particolari di dati personali (dati

sensibili) o di dati relativi a condanne penali e a reati (art. 35, commi 1 e 3 e *Considerando* 75).

Tale valutazione deve contenere almeno: una descrizione sistematica dei trattamenti previsti, delle finalità e dell'eventuale ricorrenza di un interesse legittimo; la valutazione sulla necessità e proporzionalità dei trattamenti rispetto alle predefinite finalità; la valutazione dei rischi per i diritti e le libertà degli interessati; le misure tecniche e organizzative previste e ogni meccanismo utile per la tutela dei diritti dei soggetti interessati (art. 35, c. 7).

I potenziali impatti negativi sulle libertà e i diritti degli interessati dovranno essere analizzati tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (*Considerando* 90).

All'esito di questa valutazione il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento (art. 36).

All'autorità di controllo compete, altresì, la redazione e la pubblicazione di un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati. La stessa autorità può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta la citata valutazione d'impatto (art. 35, c. 4).

Titolare e responsabile del trattamento sono tenuti, altresì, tanto alla valutazione dei rischi quanto all'adozione di misure tecniche ed organizzative, adeguate a garantire un elevato livello di sicurezza, che comprendono: la pseudonimizzazione, la cifratura, meccanismi per garantire riservatezza e integrità, ecc. (art. 32, c. 1).

Il titolare dovrà poi notificare all'autorità di controllo eventuali violazioni dei dati personali (art. 33).

Vengono inoltre istituiti i registri delle attività di trattamento da tenersi, in forma cartacea o anche in formato elettronico, a cura del titolare e del responsabile del trattamento con riferimento alle attività di trattamento svolte per conto del titolare (art. 30). Tali registri costituiscono uno strumento utile ai fini della valutazione e analisi del rischio nonché della supervisione da parte dell'autorità di controllo, alla quale dovranno essere esibiti su richiesta.

Il registro tenuto dal titolare del trattamento dovrà contenere: il nome e i dati di contatto del titolare del trattamento, e (ove applicabile) del contitolare del trattamento e del responsabile della protezione dei dati; le finalità del trattamento; una descrizione delle categorie di interessati e delle categorie di dati personali; le categorie di destinatari a cui i dati personali sono stati o saranno comunicati; (ove possibile) i termini ultimi previsti per la cancellazione delle diverse categorie di dati; (ove possibile) una descrizione generale delle misure di sicurezza tecniche e organizzative.

Il registro tenuto dal responsabile del trattamento dovrà invece comprendere: il nome e i dati

di contatto del responsabile/dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale il responsabile agisce, il responsabile della protezione dei dati (ove applicabile); le categorie di trattamenti effettuati per conto di ogni titolare del trattamento; (ove possibile) una descrizione generale delle misure di sicurezza tecniche e organizzative.

Da ultimo, al titolare e al responsabile del trattamento si affianca il responsabile della protezione dei dati, una nuova figura altamente specializzata e aggiornata, a tutela di dati e privacy, obbligatoria per le pubbliche amministrazioni.

Ogni qualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico **(4)**, il titolare e il responsabile del trattamento devono infatti procedere alla designazione di un responsabile della protezione dei dati. Lo stesso è individuato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere ai compiti di cui all'art. 39; può essere un dipendente del titolare o del responsabile del trattamento oppure un consulente esterno all'amministrazione che assolve i suoi compiti in base ad un contratto di servizi (art. 37, commi 1,5 e 6).

Qualora il titolare o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico è possibile nominare un unico responsabile della protezione per più autorità pubbliche o organismi pubblici, tenuto conto della loro dimensione e struttura organizzativa (art. 37, c. 3).

I dati di contatto del responsabile della protezione dei dati (RPD) devono essere pubblicati sul sito web dal titolare o dal responsabile del trattamento e comunicati all'Autorità di Controllo (art. 37, c. 7).

Il responsabile della protezione dei dati ha molteplici mansioni e, per questo, il Regolamento ha previsto che questo ruolo sia indipendente e abbia grande autonomia decisionale, dal momento che nessuno può fornirgli istruzioni in ordine all'esecuzione dei suoi compiti. D'altra parte egli non può svolgere altre mansioni o compiti in conflitto di interessi con quelle proprie del RDP ed è tenuto al segreto e alla riservatezza in ordine alle sue funzioni di responsabile della protezione (art. 38).

Andando ad analizzare nel dettaglio i compiti ad esso affidati, l'art. 39 individua un set minimo di funzioni che il RDP è chiamato a svolgere: informare e fornire consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dalla normativa europea e nazionale relativa alla protezione dei dati; sorvegliare l'osservanza delle disposizioni europee e nazionali in materia di privacy, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; fornire (ove richiesto) un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento; cooperare con l'autorità di controllo e fungere da punto di contatto per questioni connesse al trattamento.

Note:

(2): L'art. 4, c. 11, definisce il "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

(3): Nel Regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il *Considerando* 91 fornisce indicazioni in proposito ricomprendendovi, in particolare, "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

(4): Nel Regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo di lavoro europeo per la protezione dei dati ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico (cfr. *Linee guida sui responsabili della protezione dei dati adottate dal Gruppo Europeo per la protezione dei dati il 5 aprile 2017*).

DOSSIER
Adempimenti a carico del titolare del trattamento

Adempimenti a carico del titolare del trattamento

Il titolare è definito all'art. 4 del Regolamento come "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". Lo stesso non viene designato o nominato, ma diventa tale nel momento in cui raccoglie dati personali con l'intento di trattarli per finalità lecite, come previsto all'art. 6, e decide le modalità di trattamento.

Il titolare è responsabile del rispetto del GDPR all'interno del proprio ente e deve mettere in atto tutte le misure tecniche ed organizzative idonee a dimostrare la conformità allo stesso.

Di seguito si sintetizzano i nuovi adempimenti che il Regolamento pone a suo carico, fornendo dei suggerimenti operativi in merito al ruolo delle Regioni nel loro complesso (generalmente titolari del trattamento) e alle azioni che le AdG possono mettere in campo con specifico riferimento ai trattamenti effettuati in ambito FSE.

Punto a. **Designare un responsabile della protezione dei dati (RPD)**.

La scelta potrà ricadere su una professionalità interna all'amministrazione oppure su un consulente esterno. Nel primo caso occorrerà formalizzare un apposito atto di designazione a "responsabile della protezione dei dati"; nell'ipotesi, invece, di ricorso a soggetti esterni all'ente, la designazione costituirà parte integrante del contratto di servizi redatto in conformità all'art. 37 del Regolamento. L'atto di designazione, ove opportuno, potrà essere strutturato in conformità al modello elaborato dal Garante per la privacy.

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, i compiti (eventualmente anche ulteriori a quelli previsti dall'art. 39 del Regolamento) e le funzioni che questi sarà chiamato a svolgere in ausilio al titolare del trattamento, in conformità a quanto previsto dal quadro normativo di riferimento.

Nell'atto di designazione o nel contratto di servizi devono risultare sinteticamente 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, c. 5 del Regolamento (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, capacità di assolvere ai compiti di cui all'art. 39).

Il responsabile della protezione dei dati deve essere unico per amministrazione/ente, al fine di evitare rischi di sovrapposizioni o incertezze sulle responsabilità. Cionondimeno possono essere individuate più figure di supporto, con riferimento a settori diversi, che facciano però riferimento ad un unico soggetto responsabile sia che la scelta ricada su un soggetto interno sia che ci si avvalga di un consulente esterno. Infatti, in relazione alla particolare eterogeneità dei trattamenti di dati personali effettuati 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 Responsabile della protezione dei dati, anche operando (se del caso) quali componenti del suo gruppo di lavoro **(5)**.

Le amministrazioni potranno, d'altra parte, scegliere di avvalersi dell'opzione offerta dall'art. 37, c. 3 del Regolamento designando un unico RDP comune a diverse autorità pubbliche (es. Regione e Comuni); in tal caso bisognerà prestare particolare attenzione a che non si determini una situazione di conflitto d'interessi o che il responsabile della protezione dei dati non sia in grado di assolvere ai propri compiti. Conseguentemente, sarà opportuno che nell'atto di designazione o nel contratto il RPD fornisca adeguate garanzie per favorire efficienza e correttezza e prevenire conflitti di interesse.

I dati del RDP devono essere pubblicati sul sito web dell'Ente, esplicitati nell'informativa fornita all'interessato e comunicati all'autorità di controllo (Garante).

La prima azione del RPD, seguente alla sua nomina, è quella di analizzare i meccanismi di raccolta e conservazione dei dati in atto. Dopo aver valutato probabilità di perdite e tutti i possibili rischi, in relazione ai sistemi impiegati e alla particolare natura dei dati custoditi, egli produce un documento nel quale evidenzia anche l'eventuale necessità di un adeguamento tecnologico o di correttivi da apportare alle procedure in atto. Una volta mappata la realtà esistente, il RPD si fa carico della redazione di un piano di aggiornamento e manutenzione dei sistemi **(6)**.

Suggerimenti per le AdG FSE

Fermo restando che il RDP deve essere unico per l'Amministrazione e le AdG non hanno un ruolo al riguardo, le stesse potrebbero individuare una persona di supporto al responsabile della protezione dei dati designato a livello regionale (es. con DGR) per assisterlo nell'analisi delle procedure messe in atto per la raccolta e conservazione dei dati personali relativi ai partecipanti agli interventi cofinanziati dal FSE.

Punto b. **Predisporre e implementare un registro delle attività di trattamento.**

Il titolare del trattamento dovrà tenere un registro delle attività di trattamento effettuate sotto la propria responsabilità che contenga, ai sensi dell'art. 30, c. 1, almeno: i riferimenti del

titolare e del responsabile della protezione dei dati, le finalità del trattamento, una descrizione delle categorie di interessati e delle categorie di dati personali, le categorie di destinatari a cui i dati sono stati/saranno comunicati. Ove possibile potranno essere indicati i termini previsti per la cancellazione delle diverse categorie di dati e una descrizione generale delle misure di sicurezza tecniche ed organizzative.

Suggerimenti per le AdG FSE

Le AdG individuate come titolari del trattamento dovranno predisporre ed implementare un registro delle attività di trattamento effettuate sotto la propria responsabilità che contenga gli elementi di cui all'art. 30, c. 1 del Regolamento.

Punto c. **Effettuare un'analisi del rischio ed adottare le misure di sicurezza adeguate.**

Al fine di progettare misure tecniche ed organizzative adeguate a garantire un elevato livello di sicurezza (contro i rischi di perdita, distruzione, violazione dei dati, ecc.) le amministrazioni dovrebbero preventivamente predisporre un documento di analisi dei rischi. Ove disponibili si potrà procedere all'aggiornamento di analisi esistenti per adeguarle alle disposizioni del Regolamento UE, qualora siano stati introdotti nuovi trattamenti o siano avvenute variazioni sostanziali su quelli in essere. L'adeguatezza delle misure adottate, a protezione dei dati, potrà essere dimostrata anche facendo riferimento ad eventuali meccanismi di certificazione (ex art. 42 GDPR).

Suggerimenti per le AdG FSE

Le AdG individuate come titolari dei trattamenti dei dati relativi alle operazioni cofinanziate dal FSE dovrebbero predisporre un documento di analisi dei rischi, o aggiornare eventuali analisi esistenti, e valutare l'adeguatezza delle misure di sicurezza messe in atto per proteggere i dati.

Punto d. **Eseguire la valutazione d'impatto sulla protezione dei dati personali (DPIA).**

La DPIA deve essere condotta dal titolare, insieme al RPD e al responsabile (o ai responsabili) del trattamento nella fase di progettazione del trattamento. La sua conduzione materiale può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia, la responsabilità ultima dell'adempimento ricade sul titolare del trattamento.

Lo svolgimento di una DPIA non è obbligatorio per ogni singolo trattamento, tale valutazione è infatti necessaria solo se il trattamento "può comportare un rischio elevato per i diritti e le libertà delle persone fisiche". Una DPIA può riguardare un singolo trattamento; tuttavia come previsto dall'art. 35 del Regolamento è possibile utilizzare un'unica DPIA per valutare più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Il Regolamento individua tra le fattispecie per le quali tale valutazione è obbligatoria il trattamento, su larga scala, di dati sensibili o di natura estremamente personale (art. 35, c. 2b) nonché quelli relativi a interessati vulnerabili quali: minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc. (*Considerando 75*).

La DPIA è, d'altro canto, uno strumento importante di ausilio al titolare per dimostrare l'adozione di misure idonee a garantire il rispetto delle prescrizioni del Regolamento UE in materia di privacy. Pertanto anche laddove la necessità di una DPIA non emerga con chiarezza, il gruppo europeo per la protezione dei dati raccomanda di farvi comunque ricorso in quanto essa contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento **(8)**.

Lo stesso gruppo ha precisato, ad ogni modo, alcuni casi in cui tale valutazione non è necessaria. Tra questi si possono annoverare le ipotesi in cui: il trattamento trova la propria base legale nel diritto dell'UE o di uno Stato membro, la base legale in questione disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta (art. 35, c. 10); il trattamento è compreso nell'elenco facoltativo (redatto dall'autorità di controllo ai sensi dell'art. 35, c. 5) dei trattamenti per i quali non è necessario procedere alla DPIA **(9)**.

Per i trattamenti in corso l'obbligo di condurre una DPIA vige nel caso in cui possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e ove siano intervenute variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi.

Nelle circostanze in cui la tipologia di trattamento richiederebbe una valutazione d'impatto sulla protezione dei dati, in quanto ricorrono i presupposti previsti dal Regolamento, ma il titolare ritiene che non "può presentare un rischio elevato", egli dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando l'opinione del responsabile della protezione dei dati **(10)**.

In ordine alle modalità di realizzazione della valutazione d'impatto, il Regolamento fissa le caratteristiche basilari di una DPIA all'art. 35, c. 7 e nei *Considerando* 84 e 90. Ulteriori indicazioni si rinvengono (inoltre) nelle pertinenti linee guida, laddove l'allegato 1 contiene esempi di metodologie per la valutazione di impatto sulla protezione dei dati e sulla privacy.

Suggerimenti per le AdG FSE

In considerazione dell'ampio ventaglio di interventi supportati dal FSE destinati a gruppi particolarmente vulnerabili, che richiedono la rilevazione e il trattamento di numerosi dati anche sensibili, tenuto conto (inoltre) che la registrazione di tali informazioni avviene in linea di massima attraverso sistemi di archiviazione informatizzati, l'obbligo di procedere alla valutazione d'impatto dei rischi per i diritti e le libertà delle persone fisiche sembrerebbe (in astratto) sussistere anche per i trattamenti effettuati in ambito FSE.

Cionondimeno, alla luce delle indicazioni fornite dal Gruppo Europeo sulla protezione dei dati, tale valutazione potrebbe non essere necessaria in quanto le operazioni di trattamento effettuate in relazione agli interventi finanziati dal FSE trovano la loro base giuridica nel Diritto UE (segnatamente nel Regolamento 1304/2013) e si presume dunque che una valutazione in merito ai potenziali impatti sul diritto alla protezione dei dati dei destinatari sia già stata condotta all'atto della definizione della base giuridica suddetta.

Ad una interpretazione chiara ed univoca del disposto regolamentare, con riferimento ai trattamenti effettuati in tale ambito, si potrebbe (auspicabilmente) giungere a seguito della pubblicazione (facoltativa) da parte del garante nazionale della lista dei trattamenti esclusi

dall'obbligo di DPIA, o a fronte di un suo parere, nonché a seguito della elaborazione di eventuali guide orientative da parte del Comitato europeo per la protezione dei dati (CEPD).

Ad ogni modo, qualora si rendesse comunque necessario/opportuno procedere ad una DPIA anche per i trattamenti in ambito FSE, questa dovrebbe essere condotta dalle AdG se individuate come titolari del trattamento. Diversamente qualora l'AdG rivesta il ruolo di responsabile del trattamento dovrebbe collaborare con il titolare e il responsabile della protezione dei dati per la realizzazione della valutazione.

Note:

(5): Cfr. FAQ garante Privacy sul responsabile della protezione dei dati.

(6): Per ulteriori approfondimento in merito alla figura del responsabile della protezione dei dati confronta "Linee guida sui responsabili della protezione dei dati" elaborate dal Gruppo Europeo per la protezione dei dati ed adottate il 5 aprile 2017.
Si vedano inoltre le FAQ pubblicate sul sito web del Garante per la privacy.

(7): Cfr. "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679" adottate dal Gruppo Europeo per la protezione dei dati adottate il 4 aprile 2017 ed emendati il 4 ottobre dello stesso anno.

(8): Ibidem

(9): Ibidem

(10): Ibidem

DOSSIER
Adempimenti a carico del responsabile del trattamento

Adempimenti a carico del responsabile del trattamento

Il GDPR definisce all'art. 4 il Responsabile del trattamento come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" e ne descrive le funzioni all'art.28.

Ai fini di una corretta applicazione delle disposizioni del Regolamento risulta utile distinguere fra la funzione di "Responsabile del trattamento", così come definita all'art. 28 del Regolamento, assegnata a un soggetto esterno che esegue trattamenti per conto dell'amministrazione sulla base di un contratto/convenzione e la funzione che possiamo definire di "Responsabile interno" che nella prassi è assegnata a uffici/dipartimenti che esercitano funzioni di particolare rilievo.

Gli adempimenti che il Regolamento pone in capo al responsabile del trattamento sembrerebbero riferiti ai soggetti esterni, che eseguono trattamenti per conto del titolare, e non anche a coloro che svolgono la funzione di responsabile interno della PA. Le azioni di seguito elencate dovrebbero essere, conseguentemente, attivate dalle Regioni nel caso in cui rivestano il ruolo di responsabili esterni del trattamento (ad es. se come OI eseguono trattamenti per conto di un'altra autorità pubblica che è AdG).

Punto a. **Designare un responsabile della protezione dei dati**

Si dovrà procedere alla nomina del RPD qualora tale figura non sia stata già individuata dalle amministrazioni in qualità di titolari del trattamento dei dati. Il responsabile della protezione dei dati deve essere infatti unico per amministrazione/ente, al fine di evitare rischi di sovrapposizioni o incertezze sulle responsabilità.

Suggerimenti per le AdG

Nell'ambito delle operazioni cofinanziate dal FSE le AdG svolgono sovente le funzioni di responsabili (interni) del trattamento dei dati. In tale ipotesi esse non dovranno comunque procedere alla designazione di un RDP in quanto (come detto) tale figura deve essere un'unica per l'intera Regione.

Tale obbligo potrebbe invece sussistere per i beneficiari/attuatori, che coadiuvano l'amministrazione nella raccolta e trattamento dei dati sui partecipanti ai percorsi FSE, qualora individuati (nell'atto di adesione/convenzione) quali responsabili del trattamento. Nello specifico essi dovranno procedere alla designazione del RPD qualora siano pubbliche amministrazioni o organismi di diritto pubblico. La nomina del RDP è invece facoltativa se si tratta di soggetti privati.

Punto b. **Predisporre e implementare un registro delle attività di trattamento**

Il responsabile del trattamento dovrà tenere un registro delle attività di trattamento svolte per conto del titolare, che contenga le informazioni di cui all'art. 30, c. 2: il nome e i dati di contatto del responsabile/dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale il responsabile agisce, il responsabile della protezione dei dati (ove applicabile); le categorie di trattamenti effettuati per conto di ogni titolare del trattamento; (ove possibile) una descrizione generale delle misure di sicurezza tecniche e organizzative.

Suggerimenti per le AdG

Alla luce della funzione di "Responsabile del trattamento", così come definita all'art.28 del GDPR, le AdG qualora siano state identificate come responsabili (esterni) del trattamento dovrebbero implementare il registro delle attività di trattamento svolte per conto del titolare del trattamento (es. un'altra PA) contenente le informazioni di cui all'art. 30, c. 2.

Nel caso in cui le AdG rivestano, invece, il ruolo di "responsabili interni" il suddetto registro dovrà essere implementato dai beneficiari/attuatori, che coadiuvano l'amministrazione nella raccolta e nel trattamento dei dati relativi ai partecipanti ai percorsi FSE, in qualità di responsabili esterni del trattamento.

Tale registro è obbligatorio sia per i soggetti pubblici sia per i soggetti privati. La tenuta del registro è invece facoltativa nel caso di imprese o organizzazioni con meno di 250 dipendenti, a meno che non trattino dati sensibili o relativi a condanne penali.

Punto c. **Effettuare un'analisi del rischio ed adottare le misure di sicurezza adeguate.**

Dovrà essere allo scopo predisposto, o aggiornato se esistente, un documento di analisi dei rischi dei trattamenti effettuati per conto del titolare e adottate le misure tecniche ed organizzative adeguate a garantire un elevato livello di sicurezza.

Per dimostrare l'adeguatezza delle misure progettate/utilizzate, ai fini della protezione dei dati, si potrà fare riferimento ad eventuali meccanismi di certificazione (ex art. 42 GDPR).

Suggerimenti per le AdG

Le AdG qualora siano individuate come responsabili interni del trattamento potranno eventualmente contribuire alla redazione del documento di analisi del rischio, elaborato dalla Regione in qualità di titolare, con riferimento alle attività di trattamento operate in ambito FSE.

L'analisi del rischio dovrebbe (invece) essere effettuata dai beneficiari/attuatori, in qualità di

responsabili esterni del trattamento, allo scopo di verificare l'adeguatezza delle misure di sicurezza adottate.

DOSSIER
Adempimenti a carico delle AdG titolari o responsabili dei trattamenti FSE

Adempimenti a carico delle AdG titolari o responsabili dei trattamenti FSE

Il Regolamento oltre a prevedere nuovi adempimenti, in capo ai titolari e ai responsabili del trattamento, modifica alcune disposizioni (già previste nel Codice nazionale), suscettibili di impattare più direttamente sulle attività di competenza delle AdG. Si pensi ad esempio: all'informativa da rendere all'interessato, alla puntuale declinazione dei compiti affidati al responsabile del trattamento, all'introduzione della disciplina della contitolarità, alle misure di sicurezza tecniche ed organizzative da mettere in atto, ecc.

Per agevolare le AdG nella revisione dei sistemi e della modellistica in uso, per allinearla alle previsioni del GDPR, si riportano di seguito alcune misure che le stesse potrebbero attivare in qualità di titolari o responsabili dei trattamenti relativi al FSE. Si tratta chiaramente di iniziative solo eventuali, la cui opportunità andrà valutata in ragione delle specificità di ciascuna amministrazione.

Punto a. Aggiornare il modello per l'informativa da rendere all'interessato con gli ulteriori elementi previsti dall'art. 13 del Regolamento: i dati di contatto del responsabile della protezione dei dati, la base giuridica del trattamento, il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo, il diritto dell'interessato di ottenere la limitazione del trattamento e la portabilità dei dati nonché il diritto di presentare un reclamo all'autorità di controllo.

Punto b. Aggiornare le Convenzioni/Atti di adesione/Contratti con i quali i beneficiari/attuatori vengono individuati come responsabili (esterni) del trattamento integrandoli con le informazioni aggiuntive richieste dall'art. 28 del Regolamento: natura, durata e finalità del trattamento o dei trattamenti assegnati, categorie di dati oggetto di trattamento, misure tecniche e organizzative.

Punto c. Predisporre/aggiornare linee guida per i beneficiari per fornire indicazioni in merito

alle modalità di trattamento dei dati personali alla luce delle nuove previsioni introdotte dal Regolamento Europeo: designare un responsabile della protezione dei dati (se PA/organismi di diritto pubblico), tenere un registro delle attività di trattamento ecc. In alternativa inserire un paragrafo, o aggiornarlo ove presente, dedicato al trattamento dei dati personali nell'ambito dei manuali destinati ai beneficiari **(11)**.

Punto d. Predisporre un format di registro delle attività di trattamento effettuate dal responsabile per conto del titolare, da mettere a disposizione dei beneficiari/attuatori che in qualità di responsabili (esterni) del trattamento dovranno provvedere alla sua compilazione. Si segnala, comunque, che il Garante per la privacy sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni.

Punto e. Aggiornare eventuali Convenzioni con Organismi intermedi (se individuati come contitolari del trattamento) definendo specificamente il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati.

Punto f. Aggiornare i sistemi informativi ed i rispettivi manuali e, se del caso, le pertinenti sezioni dei SIGECO alla luce di eventuali adeguamenti tecnologici o di correttivi da apportare alle procedure in atto suggeriti dal responsabile della protezione dei dati.

Note:

(11): L'art. 28 del Regolamento prevede infatti che i dati personali siano trattati dal responsabile soltanto su istruzione documentata del titolare del trattamento.