2. PRIVACY: le figure individuate dal Regolamento.

Prosegue l'analisi del Regolamento **europeo in materia di privacy (di seguito** GDPR **) per affrontare il tema delle diverse figure individuate, i relativi requisiti ed i presupposti del conferimento dell'incarico.**

1. Il Titolare del trattamento

È sua la responsabilità in merito alla valutazione del rischio e all'organizzazione di strumenti e procedure idonei a tutelare i diritti delle persone di cui vengono trattati i dati personali e resta in capo al Titolare l'onere di provare di aver adottato misure organizzative e tecniche coerenti con le prescrizioni del Regolamento, anche con riferimento alla verifica del funzionamento delle misure di sicurezza adottate. Si rende pertanto opportuno tenere traccia delle modalità di trattamento dei dati attraverso la predisposizione del relativo Registro.

Titolare del trattamento è ad esempio l'associazione che tratta i dati dei suoi soci, nella persona del Presidente/legale rappresentante.

2. Il Responsabile del trattamento

È la persona incaricata dal Titolare del trattamento a:

1. trattare i dati,
2. supervisionare il trattamento dei dati da parte dei soggetti autorizzati;
3. implementare le misure di sicurezza;
4. tenere il Registro dei trattamenti svolti[i] sotto la propria responsabilità. L'obbligo non sussiste per le organizzazioni con meno di 250 dipendenti, salvo che il trattamento possa presentare un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa il trattamento di dati "sensibili"[ii] o giudiziari;
5. designare il Responsabile della protezione dei dati (RPD-DPO) quando obbligati o quando ritenuto opportuno conferire tale incarico.

Laddove non designato un Responsabile del trattamento dati, le sue funzioni vengono assolte direttamente dal Titolare del trattamento dei dati.

L'incarico di Responsabile deve essere attribuito con un **contratto/lettera di incarico** ad una persona che presenti "*garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento"* (81° considerando del **GDPR**).

3. Il "Responsabile della protezione dati", anche detto RPD o DPO se si utilizza l'acronimo inglese di Data Protection Officer

Questa figura rappresenta una novità nel sistema privacy ma deve essere obbligatoriamente prevista solo nei seguenti casi:

1. il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccetto le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
2. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
3. le attività **principali** del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, **su larga scala**, **di categorie particolari di dati personali** (*dati che rivelino l'origine razziale o etnica, le* ***opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale,*** *nonché trattare 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*) o di dati relativi a condanne penali e a reati.

Per quanto riguarda gli enti associativi è pertanto necessario verificare verosimilmente se si configurano, o meno, le condizioni di cui al punto 3.

Sul concetto di "***larga scala***" si rinvia al 91° considerando[iii] del GDPR e alle Linee Guida del Gruppo di Lavoro dei Garanti Privacy europei che hanno fornito una serie di elementi che andrebbero considerati per poter ricavare tale nozione, quali il numero degli interessati coinvolti, il volume dei dati trattati, la durata delle attività di trattamento o l'estensione geografica del trattamento.

Per esempio, è stato definito su larga scala il trattamento posto in essere da un singolo ospedale o da un istituto assicurativo o bancario. È stato viceversa considerato un trattamento non su larga scala quello effettuato dal singolo medico con riferimento ai dati dei relativi pazienti, così come il trattamento dei dati giudiziari da parte di un singolo avvocato.

Ne consegue che difficilmente si può affermare che una associazione di base tratti dati su larga scala, mentre una associazione nazionale potrebbe farlo.

Bisogna poi verificare se i dati trattati a livello nazionale siano riconducibili alle categorie menzionate (per esempio una associazione nazionale religiosa sicuramente tratta dati *sensibili* su larga scala) o se i c.d. dati sensibili siano trattati esclusivamente dalle proprie articolazioni territoriali (*es: un ente nazionale sportivo con articolazioni territoriali autonome potrebbe trattare solo i dati anagrafici mentre le articolazioni territoriali potrebbero trattare il certificato medico di idoneità alle attività sportive dilettantistiche*).

Chi tratta i dati **può scegliere di affidare questo incarico** anche nei casi in cui non sia tenuto per legge a farlo.

L'incarico può essere ricoperto alternativamente da:

a)un dipendente/collaboratore del titolare o del responsabile, non in conflitto di interessi;

b)un soggetto esterno;

a condizione che possieda un'approfondita conoscenza della normativa e delle prassi in materia di privacy e che possa assolvere i seguenti compiti:

a)**informare e fornire consulenza** al titolare del trattamento o al responsabile del trattamento nonché ai collaboratori che eseguono il trattamento in merito agli obblighi introdotti dalla normativa;

b)**sorvegliare** l'osservanza della normativa in materia;

c)curare la **sensibilizzazione e la formazione** del personale che partecipa ai trattamenti e alle connesse attività di controllo;

d)fornire, se richiesto e laddove previsto, un **parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento;

e)cooperare con l'autorità di controllo.

L'assunzione dell'incarico non determina l'assunzione di responsabilità personali in caso di inosservanza del **GDPR**, spettando al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del GDPR stesso (articolo 24, paragrafo 1 del GDPR). Qualora non sia nominato il Responsabile della protezione dei dati, tali compiti dovranno essere assolti dal Titolare o dal Responsabile del trattamento.

Arsea comunica n. 38 del 4/5/2018

---

[i] ex art. 30, par. 2 del GDPR

"*1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:*

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale ***o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10”.***

[ii] Ossia dati inerenti “*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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*”.

[iii] Ciò dovrebbe applicarsi in particolare ai 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, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala. Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati.

Lo staff di Arsea