Federazione Italiana Giuoco Handball

PALLAMANO
DISCIPLINA OLIMPICA

Segreteria Generale

Roma, 9 maggio 2018

Circolare n. 42/2018

Alle Società Affiliate e Aderenti
Agli atleti e tecnici
Ai Signori Consiglieri Federali
Ai Signori Revisori dei Conti
Ai Comitati e Delegazioni Regionali
Alle Delegazioni Provinciali
Ai Settori Federali
LORO INDIRIZZI

Oggetto: *Privacy & data protection (Regolamento UE n. 2016/79).*

In previsione dell'entrata in vigore del Regolamento UE in materia di privacy e protezione dei dati personali, prevista per il prossimo 25 maggio, la Federazione ha ritenuto di dover mettere a disposizione delle proprie società una nota informativa – che è stata predisposta dallo Studio Legale Musumarra – allo scopo di fornire utili elementi di conoscenza della materia.

Le società che desiderino porre quesiti di carattere generale su questo argomento (con esclusione pertanto di quelli riguardanti specifiche particolari situazioni), possono inoltrarle ad office@figh.it, facendo espresso riferimento alla presente circolare. La Federazione, sulla base degli elementi informativi acquisiti dal suddetto studio legale a fronte dei quesiti ricevuti, provvederà a realizzare un apposito spazio sul sito internet riservato alle FAQ (quesiti frequenti) sul tema della privacy, a disposizione di tutti gli affiliati ed aderenti.

Le società interessate potranno altresì – ove desiderassero invece avvalersi di una diretta consulenza ed assistenza – rivolgersi allo stesso Studio Legale Musumarra che ha formulato una propria proposta riservata agli affiliati della Federazione allegata alla presente circolare (utilizzando esclusivamente la propria e-mail federale al fine di poter

usufruire delle specifiche condizioni economiche), indirizzando le proprie comunicazioni all'indirizzo e-mail studiolegalemusumarra@yahoo.it.

La nota informativa viene allegata alla presente circolare e sarà a breve altresì disponibile, unitamente alle FAQ, cliccando su "LA FIGH" nella homepage sul sito internet www.figh.it.

Distinti saluti.

Il Segretario Generale
Adriano Ruocco

Avv. Lina Musumarra
Via G. Pisanelli, 2 - 00196 Roma
Tel. +39 0636002869 - Fax +39 063213692
studiolegalemusumarra@yahoo.it
pec: linamusumarra@legalmail.it

Roma, 4 maggio 2018

Spett.le
Federazione Italiana Giuoco Handball
Stadio Olimpico (Curva Nord)
00135 – Roma

Alla c.a. del Segretario Generale, Dott. Adriano Ruocco

via e-mail: office@figh.it

Oggetto: proposta di convenzione per servizi di consulenza e assistenza legale a favore delle società affiliate (Reg. UE 2016/679 - Privacy & Data Protection)

Facendo seguito a quanto anticipato per le vie brevi, con la presente si conferma la disponibilità da parte della sottoscritta, in qualità di titolare dello Studio Legale Musumarra, di fornire un'attività di consulenza ed assistenza a favore delle società di pallamano affiliate alla FIGH finalizzata all'aggiornamento della modulistica in uso, nonché di ogni altro adempimento necessario per l'adeguamento alla normativa introdotta dal Regolamento europeo n. 679 del 27 aprile 2016 (protezione delle persone fisiche sul trattamento dei dati personali) e alla normativa nazionale in corso di approvazione (nuovo Decreto Privacy).
Nell'ambito dell'attività richiesta, sarà nostra cura fornire alle società anche i dovuti aggiornamenti.

Per quanto concerne il compenso richiesto per il predetto supporto giuridico, tenuto conto della natura e peculiarità delle attività oggetto della presente proposta, nonché della necessità evidenziata di contenere i relativi costi, si ritiene possibile quantificarlo, per ciascuna società affiliata, in euro 1.500,00, oltre al rimborso delle spese generali (15%), Iva, Cassa Avvocati (4%) ed eventuali spese vive documentate.

Resta inteso che qualora preferiste articolare in modo diverso l'attività oggetto della presente proposta siamo a Vostra disposizione per concordare una diversa modalità.

In attesa di cortese riscontro, si inviano i più cordiali saluti.

Avv. Lina Musumarra

PRIVACY & DATA PROTECTION (REGOLAMENTO UE n. 2016/679)

NOTA INFORMATIVA

a cura di Avv. Lina Musumarra - *studiolegalemusumarra@yahoo.it*

Sommario: 1. Premessa – 2. Aspetti definitori - 3. Fondamenti di liceità del trattamento – 4. Diritto di accesso – 5. Diritto di cancellazione (diritto all'oblio) – 6. Diritto di limitazione del trattamento – 7. Diritto alla portabilità dei dati - 8. Titolare, Responsabile, Incaricato del Trattamento – 9. Approccio basato sul rischio e misure di *accountability* di titolari e responsabili – 9a. Registro dei trattamenti – 9b. Misure di sicurezza – 9c. Notifica delle violazioni di dati personali - 10. Il Responsabile della protezione dei dati (RPD-DPO - *Data Protection Officer*)

1. Premessa

Il Regolamento europeo n. 679 del 27 aprile 2016, relativo alla protezione delle persone fisiche sul trattamento dei dati personali ("**GDPR**" - *General Data Protection Regulation*), già oggi vigente ma **direttamente applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018**, contiene elementi di novità ma anche di continuità rispetto alla normativa italiana imperniata sul Testo Unico in materia di protezione dei dati personali, il D.lgs. n. 196/2003 (cd. Codice Privacy), e su numerose norme e provvedimenti emanati dall'Autorità competente – DPA – ***Data Protection Authority***, ovvero il Garante per la protezione dei dati personali.

La nuova disciplina europea è frutto di una elaborazione complessa, rivolta ad una platea ampia di destinatari (cittadini, imprese, altri enti privati e pubbliche amministrazioni), per i quali l'accesso e la relativa applicazione è tutt'altro che agevole e semplice.

La sovrapposizione delle norme europee su quelle nazionali ha posto il concreto problema di cosa delle seconde debba ritenersi abrogato dalle prime.

Il Parlamento italiano ha approvato la legge di delegazione europea (L. 25 ottobre 2017, n. 163), in cui viene contemplato anche il GDPR.

In tal senso l'art. 13 delega il Governo ad adottare, entro 6 mesi dalla data di entrata in vigore della predetta legge (ovvero dal 21 novembre 2017), uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del nuovo regolamento europeo, il quale abroga la precedente direttiva 95/46/CE.

Le prime modifiche al D.lgs. n. 196/2003 sono state apportate dalla Legge n. 167 del 20 novembre 2017 ("*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea*"), in vigore dal 12 dicembre 2017. Tra queste, per la parte di interesse, si richiama l'adozione di schemi tipo predisposti dal Garante per la nomina del responsabile del trattamento di cui all'art. 29 del Codice Privacy (*infra*).

Tra gli atti urgenti presentati dal Governo italiano figura anche lo schema di decreto legislativo recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 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, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*", approvato in via preliminare dal Consiglio dei Ministri del 21 marzo 2018, n. 75.[1]

[1] Sul punto è intervenuto il Presidente dell'Autorità Garante per la protezione dei dati personali, Antonello Soro, dichiarando la propria disponibilità ad accompagnare "*le imprese italiane e i soggetti pubblici in questo passaggio con un approccio equilibrato e pragmatico, facendo appello alla categoria della saggezza*", lasciando quindi intendere che dal 25 maggio non ci sarà alcun accanimento, cfr. A. Cherchi, *Privacy, uno spiraglio per le imprese*, Il Sole 24 Ore, 3 maggio 2018.

Lo schema in parola stabilisce che "*Le disposizioni del presente decreto entrano in vigore il 25 maggio 2018*" e che "*A decorrere dall'entrata in vigore del presente decreto, il Codice in materia di protezione dei dati personali di cui al decreto legislativo 20 giugno 2003, n. 196 è abrogato*".

La finalità perseguita è quella di adeguare il quadro normativo nazionale alle disposizioni del regolamento europeo, il quale, come già ricordato, è direttamente applicabile dal 25 maggio 2018. In particolare, la legge di delegazione europea stabilisce, all'art. 13 comma 3, i seguenti criteri: "*a) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679; b) modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679; c) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal regolamento (UE) 2016/679; d) prevedere, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679; e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse*".

Oltre a ciò, fra i principi e criteri direttivi generali di cui all'articolo 32 della legge 24 dicembre 2012, n. 23 ("*Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea*"), sono indicati quelli del "*riassetto e (del)la semplificazione normativi con l'indicazione esplicita delle norme abrogate*".

A seguito delle verifiche compiute è risultato che la maggior parte delle disposizioni del Codice Privacy è da abrogare espressamente per essere risultate incompatibili con quelle recate dal regolamento; norme che, a loro volta, sono per la maggior parte direttamente applicabili e costituiranno per il futuro il regime primario interno circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché circa la libera circolazione degli stessi dati.

Il legislatore delegato ha voluto quindi rendere evidente che la fonte di riferimento è costituita dal regolamento europeo e che non vi sono due o più testi normativi, parzialmente sovrapposti, nei quali dover cercare le disposizioni e verificare la compatibilità di volta in volta.

Si è voluto dare un segnale del cambiamento intervenuto: del passaggio dalla direttiva 95/46/CE al regolamento (UE) 679/2016.

Dopo oltre 20 anni, la disciplina della protezione dei dati personali è stata oggetto di una riformulazione non formale ma sostanziale, essendo cambiato l'approccio stesso alla materia che oggi è dominata dal principio cd. dell'***accountability*** ("responsabilizzazione").

Per quanto concerne più specificatamente il mondo sportivo vengono quotidianamente trattati miriadi di dati personali (procedure di tesseramento; statistiche personali degli atleti; dati clinici; dati pubblicati sul sito federale inerenti la giustizia sportiva, immagini, eventi, classifiche; profili sui social media; comunicazioni con i tesserati; comunicazioni alle Federazioni internazionali; accrediti per eventi e manifestazioni; dati legati ai rapporti con fornitori di servizi/consulenti, alle sponsorizzazioni e merchandising; dati riconducibili all'attività antidoping).[2]

Diventa pertanto indispensabile per gli stessi operatori del settore essere pienamente consapevoli degli adempimenti e degli obblighi connessi alla privacy, secondo la nuova disciplina introdotta dal GDPR, e del connesso rischio di incorrere in sanzioni economiche e/o penali.

Ciò determina la necessità di procedere ad un'attenta analisi e verifica delle procedure già adottate, con riferimento, in particolare, ai consensi ricevuti prima del 25 maggio, per eventualmente integrare o modificare quanto necessario. Tra i nuovi principi introdotti dal regolamento europeo, come si vedrà in seguito, vi è infatti anche quello che impone, in caso di cambiamento delle finalità del trattamento, di comunicarlo agli interessati.

2. Aspetti definitori

- ***Dato personale***: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**interessato**").

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con

[2] Non può essere, peraltro, trascurato l'obbligo di conservazione del certificato penale del casellario giudiziale, che la società sportiva/datore di lavoro, la quale intende avvalersi della collaborazione di una persona per lo svolgimento di attività organizzate, caratterizzate da contatti diretti e regolari con i minori, deve preventivamente richiedere, ai sensi del D.lgs. 4 marzo 2014, n. 39 (cfr., sul punto, anche circolare Min. Lavoro n. 9 dell'11 aprile 2014).

particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Non esiste più una definizione di dati personali "**sensibili**" o di dati personali "**giudiziari**": l'art. 9 del regolamento individua in generale le "***categorie particolari di dati personali***" nelle informazioni "*che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona fisica*".

I dati relativi alla salute vengono circoscritti dal regolamento ai "*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*".

L'art. 10 disciplina il trattamento dei "*dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza*".

- ***Trattamento***: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

- ***Automatizzazione***: secondo l'art. 2, comma 1 del GDPR, il regolamento "*si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi*". Per aversi automatizzazione occorre che, in relazione all'esecuzione di uno o più operazioni, sia interposto l'utilizzo di un elaboratore/macchina, mentre è normale – ove non evitabile – che a detto utilizzo sia associato, 'a monte' o 'a valle', l'intervento della componente umana. Per quanto attiene ai trattamenti non automatizzati, essi ricadono nel campo di applicazione del regolamento nella misura in cui i dati riguardano o sono finalizzati all'inserimento in banche dati. Non può pertanto ricondursi all'ambito di applicazione normativo il semplice appunto a mano di un nome o di un telefono, ove non sia da inserire in rubrica, ovvero l'analoga informazione destinata ad un uso momentaneo e/o isolato – ancorché trattati nell'ambito di un'attività professionale, imprenditoriale o

pubblica.[3]

- ***Titolare del trattamento***: 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.

- ***Responsabile del trattamento***: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

3. Fondamenti di liceità del trattamento

Si conferma nel GDPR che ogni trattamento deve trovare fondamento in **una idonea base giuridica**; **i fondamenti di liceità del trattamento** sono indicati all'art. 6 **e coincidono, in linea di massima, con quelli previsti attualmente dal Codice Privacy** (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).[4]

a) Consenso

Cosa cambia

Per i dati "*sensibili*" (art. 9 regolamento) il consenso **deve** essere "*esplicito*"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).[5]

Il consenso **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*" (per i dati sensibili).

Inoltre, il titolare del trattamento (art. 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Il consenso dei minori è valido a partire dai 16 anni (**il limite di età può essere abbassato fino a 13 anni**

---

[3] L. Marini, *GDPR: il nuovo regolamento europeo sulla privacy*, il Quotidiano Giuridico, 2018.

[4] Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*, edizione aggiornata, febbraio 2018, www.garanteprivacy.it.

[5] Per profilazione dell'utente si intende l'insieme di attività di raccolta ed elaborazione dei dati inerenti agli utenti di servizi (pubblici o privati, richiesti o forzosi) per suddividere l'utenza in gruppi di comportamento. Si segnalano, al riguardo, le Linee-guida in materia di profilazione e decisioni automatizzate pubblicate dal Gruppo "Articolo 29", quale organismo consultivo ed indipendente (WP 251), www.garanteprivacy.it/regolamentoue/profilazione.

dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci (art. 8).

Cosa non cambia

Il consenso **deve** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **non** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo o pre-flaggate sui moduli telematici presenti sul sito web).

Deve essere manifestato attraverso "*dichiarazione o azione positiva inequivocabile*".[6]

Il Garante per la privacy raccomanda che "*Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.*

In particolare, occorre verificare che la richiesta di consenso sia ***chiaramente distinguibile*** *da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20)*".

b) Interesse vitale di un terzo

Cosa cambia

Si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione.

c) Interesse legittimo prevalente di un titolare o di un terzo

Cosa cambia

Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **non spetta** all'Autorità ma **è compito dello stesso titolare**. Si tratta di una delle principali espressioni del principio di "*responsabilizzazione*".

Cosa non cambia

L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali

[6] Per approfondimenti, si vedano i considerando 39 e 42 del regolamento.

dell'interessato per costituire un valido fondamento di liceità.[7]

Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

d) Informativa (contenuti, tempi, modalità)

Cosa cambia

I **contenuti dell'informativa** sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice Privacy.

In particolare, il titolare **deve sempre** specificare **i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - *Data Protection Officer*)**, ove esistente;[8] la **base giuridica** del trattamento; **l'interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento; se vi sia **trasferimento di dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti**.

Il regolamento prevede anche **ulteriori informazioni** in quanto "*necessarie per garantire un trattamento corretto e trasparente*": in particolare, il titolare deve specificare il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.

Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve

---

[7] In materia di bilanciamento di interessi si richiama, Garante per la protezione dei dati personali, **provvedimento in materia di videosorveglianza - 8 aprile 2010**: "*6.2. Trattamento di dati personali per fini diversi da quelli esclusivamente personali*
***Consenso**: nel caso in cui trovi applicazione la disciplina del Codice, il trattamento di dati può essere lecitamente effettuato da privati ed enti pubblici economici solamente se vi sia il consenso preventivo dell'interessato, oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso (artt. 23 e 24 del Codice).*
Nel caso di impiego di strumenti di videosorveglianza la possibilità di acquisire il consenso risulta in concreto limitata dalle caratteristiche stesse dei sistemi di rilevazione che rendono pertanto necessario individuare un'idonea alternativa nell'ambito dei requisiti equipollenti del consenso di cui all'art. 24, comma 1, del Codice.
***Bilanciamento degli interessi**: tale alternativa può essere ravvisata nell'istituto del bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice). Il presente provvedimento dà attuazione a tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell'intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro.*
A tal fine, possono essere individuati i seguenti casi, in relazione ai quali, con le precisazioni di seguito previste, il trattamento può lecitamente avvenire pure in assenza del consenso.
***Videosorveglianza (con o senza registrazione delle immagini)**: tali trattamenti sono ammessi in presenza di concrete situazioni che giustificano l'installazione, a protezione delle persone, della proprietà o del patrimonio aziendale.*
Nell'uso delle apparecchiature volte a riprendere, con o senza registrazione delle immagini, aree esterne ad edifici e immobili (perimetrali, adibite a parcheggi o a carico/scarico merci, accessi, uscite di emergenza), resta fermo che il trattamento debba essere effettuato con modalità tali da limitare l'angolo visuale all'area effettivamente da proteggere, evitando, per quanto possibile, la ripresa di luoghi circostanti e di particolari che non risultino rilevanti (vie, edifici, esercizi commerciali, istituzioni ecc.)".

[8] Si tratta di una figura nuova nel panorama normativo italiano, con un ruolo di garanzia e di supporto al titolare del trattamento e del responsabile del trattamento, punto di riferimento per tutto ciò che attiene alla privacy, sia all'interno dell'azienda/organizzazione, sia nei rapporti esterni della stessa con le Autorità di controllo e con gli interessati.

specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

Per quanto concerne i **tempi dell'informativa**, nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta,[9] oppure **al momento della comunicazione** (**non** della registrazione) dei dati (a terzi o all'interessato).[10]

Infine, con riferimento **alle modalità**, il regolamento specifica molto più in dettaglio rispetto al Codice privacy le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee.[11]

L'informativa è data, **in linea di principio, per iscritto e preferibilmente in formato elettronico** (soprattutto nel contesto di servizi *online*),[12] anche se sono ammessi "*altri mezzi*", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1).[13]

Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "*in combinazione*" con l'informativa estesa** (art. 12, paragrafo 7).[14] Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa**,[15] anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato**.[16]

Cosa non cambia

L'informativa deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento).

---

[9] Il Garante per la Privacy raccomanda che "*Dovranno essere adottate anche le misure organizzative interne idonee a garantire il rispetto della tempistica: il termine di 1 mese è chiaramente un termine massimo*".

[10] Diversamente da quanto prevede attualmente l'art. 13, comma 4, del D.lgs. n. 196/2003 a tenore del quale "*se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione*").

[11] Si veda anche considerando 58.

[12] Si vedano art. 12, paragrafo 1, e considerando 58.

[13] Il GDPR supporta il concetto delle cd. **informative stratificate**, quali formalità sintetiche integrate da più complete informative che siano agevolmente disponibili, per es., sul sito dell'organismo sportivo o attraverso un QR code contenuto nelle comunicazioni.

[14] Si è in attesa della definizione di icone standardizzate da parte della Commissione europea.

[15] Si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo.

[16] Si veda art. 14, paragrafo 5, lettera b) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice Privacy, che rinvia al giudizio del Garante.

Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati** (compreso il diritto alla portabilità dei dati), **se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.**[17]

e) Diritti degli interessati

Cosa cambia

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fino a 3 mesi in casi di particolare complessità. **Il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.**

Spetta al titolare valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere all'interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive** (anche ripetitive) (art. 12.5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice Privacy, ovvero se sono chieste **più "*copie*" dei dati personali** nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.

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, paragrafo 1).[18]

La risposta fornita all'interessato non deve essere solo "***intelligibile***", ma anche **concisa, trasparente e facilmente accessibile**, oltre ad utilizzare un **linguaggio semplice e chiaro**.

Cosa non cambia

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Benché sia il solo titolare a dover dare riscontro** in caso di esercizio dei diritti (artt. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei

---

[17] Ogni volta che le finalità cambiano, il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore. Il Garante per la Privacy raccomanda che "*I titolari del trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento*".

[18] Si veda anche art. 15, paragrafo 3.

diritti degli interessati (art. 28, paragrafo 3, lettera e).

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni, come già ricordato. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato e quest'ultimo ha il dovere di fornirle, secondo modalità idonee.[19]

Sono ammesse **deroghe ai diritti** riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici.[20]

Il Garante per la Privacy raccomanda: "*E' opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere, per impostazione predefinita,* ***forma scritta (anche elettronica)***".

4. Diritto di accesso

Cosa cambia

L'interessato ha il diritto di ricevere **una copia dei dati** personali oggetto di trattamento (art. 15 regolamento). Fra le informazioni che il titolare deve fornire **non rientrano le 'modalità' del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché **le garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

Il Garante per la Privacy raccomanda: "*Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo e degli altri diritti, i titolari possono* ***consentire agli interessati di consultare direttamente, da remoto*** *e in modo sicuro, i propri dati personali*".

5. Diritto di cancellazione (diritto all'oblio)

Cosa cambia

Il diritto cosiddetto all'oblio (art. 17 regolamento) si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno reso pubblici i dati

[19] Si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6.
[20] Si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"*oblio*", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica.

personali dell'interessato, ad es., pubblicandoli su un sito web) di **informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati**, compresi "*qualsiasi link, copia o riproduzione*".

Rispetto all'art. 7, comma 3, lett. b) del Codice Privacy, il diritto all'oblio ha **un campo di applicazione più esteso**, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati (per esempio, anche dopo la revoca del consenso).

6. Diritto di limitazione del trattamento

Cosa cambia

Si tratta di un diritto **diverso e più esteso rispetto al "blocco" del trattamento** di cui all'art. 7, comma 3, lett. a) del Codice Privacy: in particolare, è esercitabile **non solo in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche **se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento**, *ex* art. 21 del regolamento (in attesa della valutazione da parte del titolare).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento dei diritti in sede giudiziaria, tutela dei diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Il Garante per la Privacy raccomanda: "*Il diritto alla limitazione prevede che **il dato personale sia 'contrassegnato'** in attesa di determinazioni ulteriori; pertanto è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo*".

7. Diritto alla portabilità dei dati

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (ad esempio, la portabilità del numero telefonico).

Cosa cambia

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e

sono previste specifiche condizioni per il suo esercizio. In particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare) e solo i dati che siano stati ***"forniti"* dall'interessato** al titolare.

Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili ad un altro titolare indicato dall'interessato, se tecnicamente possibile.[21]

8. Titolare, Responsabile, Incaricato del Trattamento

Cosa cambia

Il regolamento: a) 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; b) fissa più dettagliatamente (rispetto all'art. 29 del Codice Privacy) 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) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "*garanzie sufficienti*" (quali, in particolare, la 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); c) consente **la nomina di sub-responsabili del trattamento** da parte di un responsabile,[22] per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario. Quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "*non gli è in alcun modo imputabile*";[23] d) prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in

[21] Si rinvia per maggiori approfondimenti a www.garanteprivacy.it/regolamentoue/portabilita.
[22] Si veda art. 28, paragrafo 4.
[23] Si veda art. 82, paragrafo 1 e paragrafo 3.

particolare, la tenuta del **registro dei trattamenti** svolti (*ex* art. 30, paragrafo 2); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (*ex* art. 32 regolamento); la **designazione di un RPD-DPO** nei casi previsti dal regolamento o dal diritto nazionale.[24]

Si ricorda, inoltre, che **anche il responsabile** non stabilito nell'UE dovrà **designare un rappresentante in Italia** quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento.[25]

Cosa non cambia

Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice Privacy italiano).

Pur non prevedendo espressamente **la figura dell' "*incaricato*" del trattamento** (*ex* art. 30 Codice Privacy), 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*".[26]

Il Garante per la Privacy raccomanda: "*I titolari di trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del regolamento. Dovranno essere apportate le necessarie integrazioni o modifiche, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti*". Sottolinea, altresì, il Garante: "*Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante*".

---

[24] Si veda art. 37 del regolamento.

[25] Diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice Privacy, a tenore del quale "*Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali*".

[26] Si veda, in particolare, art. 4, n. 10, del regolamento.

9. Approccio basato sul rischio e misure di *accountability* di titolari e responsabili

Cosa cambia

Nell'ambito del principio di responsabilizzazione - che si sostanzia **nell'adozione di comportamenti proattivi** e **tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** - viene 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 in forza di alcuni criteri specifici.

Il primo fra tali criteri, sintetizzato dall'espressione inglese "***data protection by default and by design***" (art. 25 regolamento), determina la necessità di configurare il trattamento prevedendo sin dall'inizio le garanzie indispensabili. Per fare ciò si richiede un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili**.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati;[27] tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35-36 regolamento),[28] 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.[29]

All'esito di questa valutazione di impatto 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.

Dunque, l'intervento delle autorità di controllo sarà principalmente *ex post*, ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; **ciò spiega l'abolizione a partire**

---

[27] Si vedano considerando 75-77.
[28] Si vedano artt. 35-36.
[29] La CNIL, l'Autorità francese per la protezione dei dati, ha messo a disposizione un software di ausilio ai titolari in vista dell'effettuazione della valutazione d'impatto sulla protezione dei dati (DPIA), la cui versione in lingua italiana è stata messa a punto anche con la collaborazione del Garante per la Privacy, consultabile in http://www.garanteprivacy.it/web/guest/home/docweb.

dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice privacy italiano, come la **notifica preventiva dei trattamenti** all'autorità di controllo e il cd. ***prior checking*** (o verifica preliminare, art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

Peraltro, alle autorità di controllo, e in particolare al "*Comitato europeo della protezione dei dati*" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

9a. Registro dei trattamenti

Cosa cambia

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30 del regolamento. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante per la Privacy, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di una azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Il Garante per la Privacy raccomanda: "*La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì* ***parte integrante di un sistema di corretta gestione dei dati personali****. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti*".

9b. Misure di sicurezza

Cosa cambia

Le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento (art. 32, paragrafo 1 del regolamento). In questo senso **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva**. Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "*minime*" di sicurezza** (*ex* art. 33 Codice Privacy) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificatamente individuati come da art. 32 del regolamento. Il Garante per la Privacy richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Potranno inoltre restare in vigore (in base all'art. 6, paragrafo 2 del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili.[30]

9c. Notifica delle violazioni dei dati personali

Cosa cambia

A partire dal 25 maggio 2018 **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene attualmente – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "*senza ingiustificato ritardo*", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati. Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "*senza ingiustificato ritardo*".

Il Garante per la Privacy raccomanda: "*Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33,*

[30] E' il caso, in particolare, dei trattamenti di dati sensibili svolti da soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (artt. 20 e 22 Codice Privacy), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice" (Privacy).

10. Il Responsabile della protezione dei dati (RPD-DPO - *Data Protection Officer*)

Cosa cambia

La designazione di tale nuova figura riflette l'approccio responsabilizzante che caratterizza il regolamento europeo, essendo finalizzata a facilitare l'attuazione dello stesso da parte del titolare/responsabile. Non è un caso, infatti, che tra i compiti del DPO rientrino "*la sensibilizzazione e la formazione del personale*" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35, già richiamato. La sua designazione **è obbligatoria**, per le aziende private, se l'attività principale consiste nel **monitoraggio regolare e sistematico degli interessati su larga scala**, oppure nel trattamento su larga scala di categorie particolari di dati personali (quelli sensibili) o relativi a condanne penali e reati (art. 37 del regolamento).

Secondo le Linee Guida pubblicate dal Gruppo Articolo 29, per "*attività principale*" si intendono le operazioni essenziali al raggiungimento degli obiettivi perseguiti dall'azienda; per "*trattamento sistematico su larga scala* ci si riferisce a tutte le forme di tracciamento, profilazione o monitoraggio, sia su internet, ma anche al di fuori del contesto *online.* I criteri da tenere in considerazione per valutare se un trattamento rientra in questa categoria sono: a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c) la durata, ovvero la persistenza, dell'attività di trattamento; d) la portata geografica dell'attività di trattamento.

Una volta verificata la necessità di nominare il DPO, si dovrà procedere alla scelta della figura (interna o esterna) o, in alternativa, **a documentare le valutazioni condotte per determinare che la società non è tenuta a tale nomina**. E' comunque incoraggiata esplicitamente nelle Linee Guida **la designazione** di un Responsabile della protezione dei dati su **base volontaria** per ragioni di organizzazione interna. Secondo quanto previsto dall'art. 38 del regolamento, il DPO deve agire in modo autonomo, la sua posizione deve essere indipendente rispetto alle altre funzioni dell'azienda. Non sono previsti albi o altri organismi professionali per tale figura, dovendo possedere qualità professionali adeguate alla complessità dei

trattamenti di dati posti in essere dall'azienda e a tal fine dovrà essere selezionato tra figure con competenze tecnico-legali e con esperienza in materia di protezione dei dati. Sul punto il Garante per la Privacy ha affermato che eventuali certificati, rilasciati al termine di un percorso formativo, sebbene costituiscano "*un valido strumento ai fini della verifica del possesso di un livello minimo di conoscenza della disciplina, tuttavia non equivalgono, di per sé, a una 'abilitazione' allo svolgimento del ruolo del RPD*".[31]

A differenza dei responsabili interni del trattamento dei dati nominati secondo il Codice Privacy, il DPO **non è un delegato del titolare del trattamento**. Ha esclusivamente un ruolo consultivo e di garanzia, come delineato dai compiti minimi elencati dall'art. 39 del regolamento.

Nel caso di DPO esterno, ai sensi dell'art. 37, paragrafo 6, la nomina avviene per mezzo di un **contratto di servizi**.[32]

[31] Provv. 28.7.2017.
[32] Il Garante per la Privacy ha reso disponibile un modello di atto di designazione, consultabile sul sito www.garanteprivacy.it/regolamentoue/rpd.