Deloitte.
Legal

Data Protection | *Breaking news*

Il DPO: nomina o non nomina?

Marzo 2022

Il DPO: nomina o non nomina?

Il **Data Protection Officer (DPO)** è una **figura chiave in materia di privacy**.
Nonostante il GDPR preveda una specifica norma relativa alla nomina di tale figura, non è sempre chiaro quando tale obbligo debba essere attuato.
L'EDPB e alcune Autorità di controllo europee hanno rilasciato alcune linee guida per aiutare le organizzazioni pubbliche e private nello svolgimento di tale valutazione. Sono state anche emesse diverse sanzioni in materia.

PRINCIPALI FONTI

- Gdpr e Codice Privacy
- Linee-guida sui Responsabili della Protezione dei Dati del Gruppo di Lavoro art. 29
- FAQ del Garante per la Protezione dei Dati Personali sul Responsabile della Protezione dei Dati in ambito pubblico
- FAQ del Garante per la Protezione dei Dati Personali sul Responsabile della Protezione dei Dati in ambito privato
- Practical Guide GDPR – Data Protection Officer del CNIL

I casi di nomina obbligatoria del DPO

Ai sensi dell'**art. 37 GDPR**, la designazione del DPO è obbligatoria ogniqualvolta:

1. il trattamento è svolto da un'**autorità pubblica** o da un **organismo pubblico**;
2. le **attività principali** del titolare o del responsabile consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico** di interessati su **larga scala**;
3. le **attività principali** del titolare o del responsabile consistono nel **trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e reati.**

Lo scopo del presente breve documento è fornire alcune **precisazioni** ed **esempi** collegati ai suddetti criteri.

Autorità e organizzazioni pubbliche

Si intendono non solo le **autorità nazionali, regionali e locali**, ma anche altre organizzazioni pubbliche come gli **istituti di istruzione superiore, gli ospedali, le aziende del Servizio sanitario nazionale, le Camere di commercio, le autorità amministrative indipendenti,** ecc.

Il Codice Privacy (art. 2-*sexiedecies*) prevede inoltre che siano obbligate alla nomina del DPO le **autorità giudiziarie nell'esercizio delle loro funzioni**.

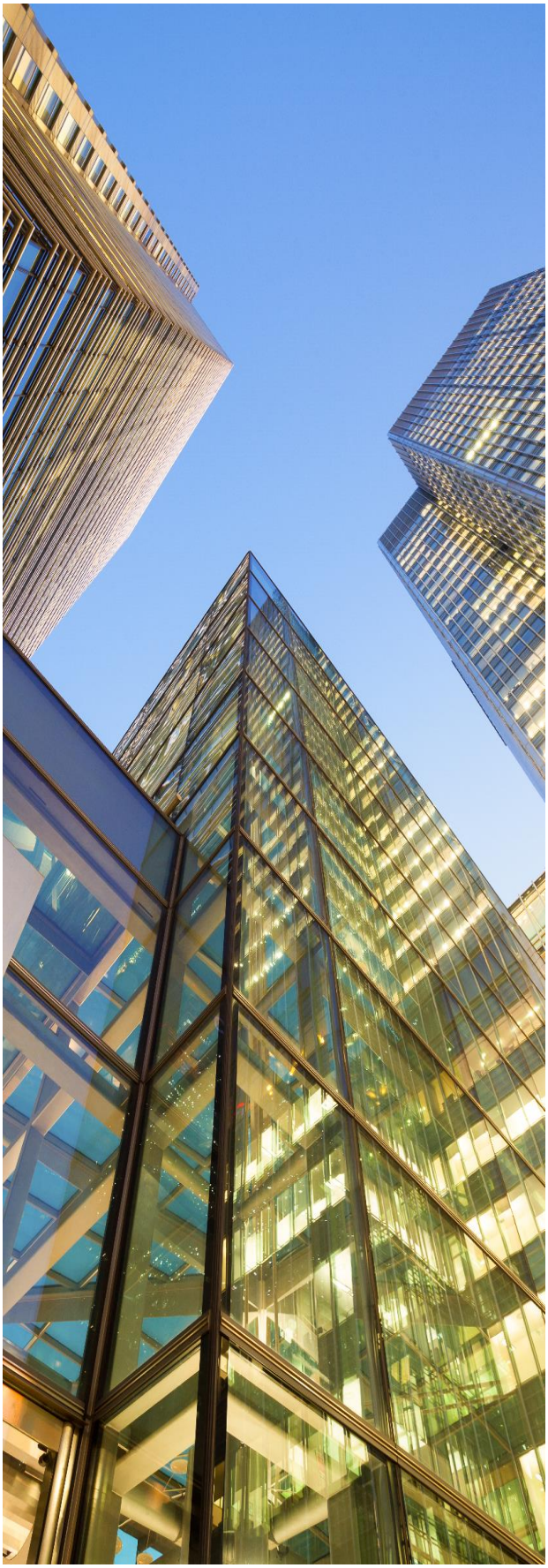
Best practice

Le organizzazioni private incaricate di un compito di servizio pubblico (e.g. concessionari di servizi pubblici) mantengono il loro status di diritto privato e non sono quindi tenute a nominare un DPO.

Tuttavia, la designazione di un DPO è incoraggiata per questi enti. Si pensi, ad esempio, agli ordini professionali, ai fornitori del servizio radio-televisivo pubblico, di servizi di trasporto pubblico, di somministrazione di acqua, energia, gas, ecc.

«Attività principali»

L'attività principale di un'organizzazione corrisponde al suo **core business**. Ove il trattamento dei dati sia **inscindibilmente connesso allo svolgimento delle operazioni essenziali e necessarie al raggiungimento degli obiettivi dell'organizzazione**, allora tale attività di trattamento del titolare o del responsabile può considerarsi «principale».



Ad,esempio, il **trattamento di dati relativi alla salute** (come le cartelle cliniche dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale. Pertanto, il trattamento di tali dati deve, in questo caso, essere considerato attività principale della struttura, dunque tutti gli ospedali sono tenuti a designare un DPO.

Tuttavia, si consideri che le **attività di supporto o ausiliarie** (e.g., la retribuzione dei dipendenti o il supporto informatico), pur essendo necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, sono considerate solo di **natura accessoria** e non attività principali.

Trattamento su «larga scala»

Non esiste una soglia applicabile a tutte le situazioni oltre la quale un trattamento è considerato su «larga scala». Per valutare tale criterio è quindi necessaria un'**analisi caso per caso**, che deve considerare un insieme di fattori, tra cui:

- il **numero di interessati** (in termini assoluti ovvero espressi in percentuale rispetto alla popolazione di riferimento);
- il **volume** dei dati e/o le diverse **tipologie** di dati oggetto di trattamento;
- la **durata** dell'attività di trattamento;
- la **portata geografica** dell'attività di trattamento.

Di seguito alcuni esempi di **trattamento su larga scala**:

- trattamento di dati relativi agli spostamenti di utenti di un **servizio di trasporto pubblico cittadino** (e.g. il loro tracciamento attraverso titoli di viaggio);
- trattamento di **dati di geolocalizzazione** raccolti in tempo reale, **per finalità statistiche** (e.g. rispetto ai clienti di una catena internazionale di fast food);
- trattamento di dati relativi alla clientela da parte di una **compagnia assicurativa** o di una **banca** nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di **pubblicità comportamentale/profilata**;
- trattamento di dati (e.g. metadati, contenuti, ubicazione) da parte di fornitori di **servizi telefonici o telematici**;
- trattamento di dati da parte di una **società di revisione contabile**;
- trattamento di dati da parte di **istituti di vigilanza**;
- trattamento di dati da parte di **partiti e movimenti politici**;
- trattamento di dati da parte di **imprese di somministrazione di lavoro e ricerca del personale**;
- trattamento di dati da parte di **società di call center**;
- trattamento di dati da parte di **sindacati, CAF e patronati.**

Alcuni esempi di trattamento **non** su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un **singolo professionista sanitario**;
- trattamento di dati personali relativi a condanne penali e reati svolto da un **singolo avvocato**;
- trattamento di dati da parte di **amministratori di condominio**;
- trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti **da parte di imprese individuali o familiari o PMI**.

«Monitoraggio regolare e sistematico»

Tale concetto comprende tutte le **forme di tracciamento** e **profilazione** su Internet anche per finalità di pubblicità comportamentale. Non si tratta, però, di un'attività riferita esclusivamente all'ambiente online. Di seguito alcuni elementi che possono aiutare a chiarire.

L'aggettivo «**regolare**» ha almeno uno dei seguenti significati relativi al monitoraggio:

- che avviene in modo continuo o a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo «**sistematico**» ha almeno uno dei seguenti significati relativi al monitoraggio:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcuni **esempi** di attività di monitoraggio regolare e sistematico:

- prestazione di servizi di **telecomunicazioni**;
- reindirizzamento di messaggi di posta elettronica;
- attività di **marketing basate sull'analisi dei dati raccolti**;
- profilazione e scoring per finalità di **valutazione del rischio**;
- **geolocalizzazione** (e.g. svolta da parte di app su dispositivi mobili);
- programmi di **fidelizzazione**;
- **pubblicità comportamentale**;
- **monitoraggio** di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla **salute** attraverso **dispositivi indossabili**;
- utilizzo di **telecamere** a circuito chiuso;
- dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

Best practice

La designazione di un DPO è raccomandabile anche in casi ulteriori rispetto a quelli precedentemente elencati. Infatti, anche ove la nomina non sia strettamente prevista, può risultare opportuno procedere a tale designazione su base volontaria, anche alla luce del **principio di accountability**.

Tale designazione è **raccomandata, tra l'altro, anche nei casi in cui l'organizzazione riscontri difficoltà relative alla protezione dei dati personali**; ciò permette di affidare la gestione delle criticità a un esperto per l'identificazione e il coordinamento delle azioni da intraprendere.

Alcune recenti sanzioni delle Autorità di controllo europee

In **Italia** il Garante Privacy ha sanzionato, nel 2021, due società che operano nell'ambito del food delivery, **Foodinho S.r.l.** e **Deliveroo Italy S.r.l.**:

- nel primo caso, per **non aver posto in essere le attività necessarie alla nomina di un proprio DPO** e **non aver sollecitato la società capogruppo a comunicarle i dati di contatto del DPO di gruppo** da inserire nell'informativa ex art. 13 GDPR;

- nel secondo caso, in ragione della **mancata designazione** da parte della società Deliveroo del DPO e della **mancata comunicazione della suddetta designazione all'Autorità di controllo competente**.

Nel caso di specie, la designazione obbligatoria del DPO è stata valutata sulla base dei seguenti criteri:

- la **portata geografica** dell'attività di trattamento (il servizio è diffuso in più di 200 città nel mondo);
- il **numero di interessati** che utilizzano l'App;
- la **profilazione** degli utenti;
- il trattamento di molteplici tipologie di dati personali, quali **dati di geolocalizzazione, dati relativi alle abitudini alimentari e di consumo**, nonché **dati appartenenti a categorie particolari** (e.g. allergie e intolleranze alimentari).

L'Autorità di controllo spagnola (AEPD) ha sanzionato nel 2020 per 50 mila euro Conseguridad SL, società di **sicurezza privata**, che aveva installato un **impianto di videosorveglianza** in grado di riprendere qualsiasi soggetto presente negli stabilimenti.

L'AEPD ha ritenuto che la mancata nomina del DPO sia da considerarsi una violazione del GDPR, nella misura in cui il trattamento dei dati svolto dalla società richiede per sua natura, ambito di applicazione e/o finalità, il **monitoraggio regolare e sistematico degli interessati su larga scala**.

Un'altra sanzione di importo pari a 25 mila euro dell'**Autorità spagnola** è quella comminata nel 2019 alla società **Glovoapp23 SL**.

L'**Autorità di controllo belga** ha sanzionato nel 2022 **IAB Europe A.I.S.B.L.**, società di erogazione di contenuti e **annunci pubblicitari online**, anche a causa della mancata nomina del DPO.

L'**Autorità di controllo tedesca** ha sanzionato nel 2019 il fornitore di servizi di telecomunicazioni **Telecom GmbH** per la mancata nomina del DPO. La sanzione ammonta a soli 10 mila euro.

Experience the future of law, today

Today, you need smart lawyers who bring even more to the table than legal advice and memorandums. You need to work better, faster and with lower total cost. That takes someone who knows your business and your industry, yet thinks and works in new ways. A steady hand at the center of the transformation all around us. An expert in law, commerce and technology, who is able to serve you globally.

To make an impact that matters, you need an accomplished confidante who is both pragmatic and pioneering.

Deloitte Legal invites you to experience the future of law, today. Meet current obligations more effectively while anticipating future opportunities.

Automate complicated and time-consuming legal activities. Benefit from a commercial mindset that integrates legal, business and industry expertise. Draw upon our experience with business operating model transformation.

As you lead your enterprise through unprecedented complexity and change, we'll work with you not just for you. Working together, you're empowered to make confident decisions, guide your business and take advantage of possibilities.

Experience the future of law, today.

Key contacts Data Protection Team

Ida Palombella

Partner

ipalombella@deloitte.it

Pietro Boccaccini

Director

pboccaccini@deloitte.it

Simone Prelati | Federico Vota

Camilla Torresan | Lidia Letterelli | Benedetta Antonelli

Deloitte.
Legal