Circolare del 23 febbraio 2021

INDICE

PRIVACY, IL GARANTE SANZIONA MINISTERO DELLO SVILUPPO ECONOMICO E REGIONE LAZIO

Il primo per non aver nominato il Responsabile della Protezione dei Dati, e la seconda per non aver designato il Responsabile del trattamento (provvedimenti nn. 9/2021 e 54/2021)

Con i provvedimenti n. 54 dell'11 febbraio 2021 e n. 9 del 14 gennaio 2021, l'Autorità focalizza la propria attenzione sulla Pubblica Amministrazione, sanzionando alcune inadempienze palesi (come la mancata nomina del RDP/DPO) e andando a chiedere conto della mancata nomina di un responsabile del trattamento ai sensi dell'art. 28 del GDPR.

Il provvedimento n. 54 dell'11 febbraio 2021 nei confronti del Ministero dello Sviluppo Economico (MISE)

Nel primo dei due provvedimenti in commento (provvedimento n. 54/2021, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9556625), il Garante privacy ha emesso una ordinanza di ingiunzione del valore di 75.000 € nei confronti del M.I.S.E. per non avere nominato il Responsabile della Protezione Dati (RPD / DPO) entro il 25 maggio 2018, data di piena applicazione del Regolamento Europeo 679/2016 (GDPR) e per avere diffuso sul sito web istituzionale informazioni personali di oltre 5000 manager.

L'Autorità ha sanzionato una Pubblica Amministrazione per non avere designato il RDP entro il termine stabilito e per avere provveduto alla nomina e alla comunicazione al Garante dei dati di contatto con notevole ritardo. Ciò nonostante il Garante avesse, fin dal maggio 2017, avviato una articolata attività informativa rivolta a tutti i Ministeri, indicando proprio la nomina del RPD tra le priorità da tenere in considerazione nel percorso di adeguamento al nuovo quadro giuridico.

La sanzione in commento è di particolare importanza in riferimento all'obbligo stabilito dall'art. art. 37 comma 1 lett. a) GDPR che nella realtà delle Pubbliche Amministrazioni italiane in molti casi è ancora rimasto lettera morta. Vi è infatti un numero consistente di esse che ha provveduto in ritardo a nominare il DPO (o che non ha provveduto affatto).

Il provvedimento n. 9 del 14 gennaio 2021 nei confronti della Regione Lazio e della Cooperativa Capodarco

Il secondo dei provvedimenti in commento (n. 9/2021, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9542113) riguarda la sanzione comminata alla Regione Lazio per 75.000 euro per non aver nominato responsabile del trattamento dati la Società Cooperativa Capodarco, a cui l'Ente aveva affidato la gestione delle prenotazioni delle prestazioni sanitarie, attraverso il call center regionale (ReCUP).

Il Garante privacy ha quindi stabilito che la società ha trattato i dati dei pazienti in modo illecito per un decennio, dal 1999 al 7 gennaio 2019, data in cui la Regione Lazio, in qualità di Titolare, ha designato formalmente la Cooperativa responsabile del trattamento, ben oltre l'inizio di piena applicazione del GDPR.

Con questo secondo provvedimento, il Garante ha ribadito che le società che prestano servizi per conto del Titolare e che di conseguenza trattano i dati personali degli utenti, devono essere designate Responsabili del trattamento. Il rapporto tra Titolare e Responsabile deve essere regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, prevede nel dettaglio le regole e i limiti con cui devono essere trattati i dati personali. Il responsabile è, pertanto, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del Titolare".

Inoltre, come recentemente evidenziato dall'EDPB, il Comitato che riunisce le Autorità di protezione dati dell'UE, l'assenza di una chiara definizione del rapporto tra Titolare e Responsabile può sollevare il problema della mancanza di base giuridica su cui ogni trattamento deve fondarsi: ad esempio, per quanto riguarda la comunicazione dei dati tra Titolare e Responsabile.

Rilevato l'illecito, l'Autorità ha multato la Regione per 75.000 euro ed ha applicato la sanzione accessoria della pubblicazione del provvedimento sul sito dell'Autorità, invece nei riguardi della Cooperativa il Garante si è limitato ad una semplice ammonizione poiché quest'ultima aveva più volte rappresentato alla Regione la necessità di essere nominata responsabile del trattamento e messo in atto misure conformi al GDPR, istituendo, ad esempio, il Registro dei trattamenti.

Dalla lettura di entrambe queste sanzioni, emerge come l'Autorità amministrativa indipendente abbia preso posizione sull'organizzazione in tema privacy delle Pubbliche Amministrazioni.

L'attività istruttoria del Garante privacy

La prima delle due sanzioni ha avuto ad oggetto la nomina di una figura interna all'Ente, quale il Responsabile Protezione Dati, considerata strategica nell'attuare i principi di cui al GDPR.

Di conseguenza, nonostante le giustificazioni fornite, il Garante ha ritenuto di sanzionare il Ministero per il ritardo (un anno e mezzo circa) col quale quest'ultimo ha comunicato la nomina del RPD. Ciò nonostante il Garante avesse espressamente indicato alle Amministrazioni Pubbliche le priorità che avrebbero dovuto tenere in considerazione nel percorso di adeguamento al nuovo quadro giuridico del Regolamento; al primo posto di tale priorità era riportata proprio la designazione del Responsabile della Protezione dei Dati (artt. 37-39 GDPR), evidenziando che "questa nuova figura che il Regolamento richiede sia individuata in funzione delle qualità professionali e della conoscenza specialistica della normativa e della prassi in materia di protezione dati costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione" e che "il diretto coinvolgimento del RPD in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, è sicuramente garanzia di qualità del risultato del processo di adeguamento in atto".

Si tratta di un provvedimento in qualche modo atteso e che potrebbe preludere ad una verifica a tappeto di tutte le pubbliche amministrazioni italiane hanno nominato il ritardo il loro dopo (o non l'hanno nominato affatto).

Tale verifica sarebbe peraltro di semplice effettuazione, potendo il Garante confrontare l'elenco delle autorità o organismi pubblici che hanno comunicato nomine e variazioni dei nominativi e dati di contatto dei DPO con tutte le Pubbliche Amministrazioni italiane, come tali soggette a tale obbligo.

Con il secondo provvedimento, il Garante ha reputato che la Regione Lazio abbia effettuato un trattamento di dati personali degli interessati nell'ambito del servizio di prenotazioni sanitarie ReCUP in violazione della disciplina in materia di protezione dei dati personali e, in particolare, degli artt. 5 e 28 del GDPR.

Il Garante ha rappresentato che il Titolare è il soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati nonché una "responsabilità generale" sui trattamenti posti in essere (v. art. 5, par. 2 c.d. "accountability" e 24 del Regolamento), anche quando questi siano effettuati da altri soggetti "per suo conto" (cons. 81, artt. 4, punto 8) e 28 del Regolamento) (provvedimento del 17 settembre 2020, doc. web n. 9461168).

Nel provvedimento in commento è stato precisato che il rapporto tra Titolare e Responsabile è regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, consente al titolare di impartire istruzioni al responsabile e prevede, in dettaglio, quale sia la materia disciplinata, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare. Il Responsabile del trattamento è, pertanto, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare" (art. 28, par. 3, lett. a) GDPR).

Se ne deve dedurre che in assenza di un siffatto contratto il fornitore abbia dunque trattato i dati dei pazienti in modo illecito per un decennio, ovvero fino al 7 gennaio 2019, quando la Regione Lazio, in qualità di Titolare, ha designato formalmente la Cooperativa responsabile del trattamento, ben oltre l'inizio di piena applicazione del Regolamento europeo in materia di protezione dei dati personali.

La logica conseguenza dell'assenza di una chiara definizione del rapporto tra il Titolare e il Responsabile, come recentemente evidenziato dal Comitato Europeo per la Protezione dei Dati, può sollevare il problema della mancanza di base giuridica su cui ogni trattamento dovrebbe basarsi, ad esempio, per quanto riguarda la comunicazione dei dati tra il titolare e il presunto Responsabile (Guidelines 07/2020 on the concepts of controller and processor in the GDPR -Version 1.0- Adopted on 02 September 2020, punto 101, nota 35).

La sanzione comminata alla Regione Lazio (peraltro mitigata dalla circostanza che l'Autorità ha tenuto conto della fase di prima applicazione delle disposizioni sanzionatorie ai sensi dell'art. 22, comma 13, del D.Lgs. 10/08/2018, n. 101) per la violazione degli artt. 5, par. 2, lett. a) e 28 del Regolamento non ha coinvolto la società cooperativa.

È questo l'altro elemento che merita adeguata evidenza: ossia la circostanza per cui Il Garante ha tenuto indenne rispetto ad eventuali sanzioni il titolare della Cooperativa perché la Società Capodarco aveva più volte rappresentato alla Regione la necessità di essere nominata responsabile del trattamento e messo in atto misure conformi alla disciplina privacy, istituendo, ad esempio, il registro dei trattamenti.

Conclusioni

Dalla lettura combinata di questi due provvedimenti se ne deve dedurre che il Garante ha inteso sanzionare due Amministrazioni centrali per essere inadempienti nei confronti di due obblighi normativi stabiliti dal GDPR: la nomina del RPD e la necessità di contrattualizzare tutti i Responsabili del trattamento, che per esperienza comune non sempre sono rispettati dalle Pubbliche Amministrazioni italiane.

La funzione nomofilattica esercitata dal Garante privacy con questi due provvedimenti dovrebbe, pertanto, indurre le Pubbliche Amministrazioni a porre in essere ogni più opportuno adempimento per evitare l'applicazione di pesanti sanzioni (che oggi non avrebbero neppure il beneficio della fase di prima applicazione delle disposizioni sanzionatorie ai sensi dell'art. 22, comma 13, del d.lgs. 10/08/2018, n. 101) ed, allo stesso tempo, incoraggiare i comportamenti virtuosi di tutte quelle aziende che trattano dati per conto del Titolare che, avendo applicato correttamente i principi di cui al GDPR (nel caso concreto avendo censito i trattamenti di dati personali, anche relativi alla salute, raccolti in occasione della predetta attività di call center nel Registro delle attività di trattamento ex art. 30 GDPR e avendo designato un DPO) vedranno certamente valutati con favore questi elementi, in caso di apertura di un'istruttoria del Garante privacy.