CONFINDUSTRIA

Rassegna provvedimenti e indicazioni in materia di protezione dei dati personali

Nota di Aggiornamento

22 marzo 2021

Sommario

1. Premessa

Negli ultimi mesi, il Garante privacy ha adottato dei provvedimenti e fornito delle indicazioni su diverse tematiche di interesse per le imprese.

Di seguito, una rassegna delle questioni principali trattate dall'Autorità.

2. Organigramma e ruoli privacy

2.1 Il rapporto tra Titolare e Responsabile del trattamento

Con il **provvedimento 14 gennaio 2021, n. 9**[1], il Garante privacy ha sanzionato la Regione Lazio per **non aver nominato responsabile del trattamento** la società esterna a cui l'Ente aveva affidato il servizio di *call center* per le prenotazioni delle prestazioni sanitarie.

In particolare, l'Autorità ha ribadito che, *a fini del rispetto della normativa in materia di protezione dei dati personali, occorre identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, in particolare quella di titolare e di responsabile del trattamento e dei soggetti che operano sotto la diretta responsabilità di questi* (art. 4, par. 1, punto 7 del GDPR e artt. 28 e 29 del Codice privacy).

Al riguardo, in continuità con i precedenti pronunciamenti (v. provvedimento del 17 settembre 2020; provvedimento 10 ottobre del 2013), è stato precisato 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. artt. 5, par. 2 e 24 del GDPR), anche quando questi siano effettuati da altri soggetti "per suo conto", vale a dire i responsabili del trattamento (cons. 81, artt. 4, punto 8) e 28 del GDPR);
- le società, che prestano servizi per conto del titolare e che, di conseguenza, trattano i dati personali, 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, 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. Con la conseguenza che il responsabile del trattamento è legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare" (art. 28, par. 3, lett. a) del GDPR).
- l'assenza di una chiara definizione del rapporto tra il titolare e il responsabile 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.

[1] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9542113.

Rilevata la mancata designazione a responsabile del trattamento della Società fornitrice del servizio di *call center* per le prenotazioni delle prestazioni sanitarie, il Garante privacy ha:

- dichiarato l'illiceità del trattamento di dati personali effettuato dalla Regione Lazio che ha, infatti, consentito alla predetta Società di effettuare operazioni di trattamento dei dati in assenza di un idoneo presupposto di liceità;
- applicato la sanzione amministrativa pecuniaria di euro 75.000 e quella accessoria della pubblicazione del provvedimento sul sito dell'Autorità.

2.2 La nomina del DPO

Con il **provvedimento 11 febbraio 2021, n. 54**[2], il Garante privacy ha, tra l'altro, sanzionato il Ministero dello sviluppo economico per **non avere nominato, essendovi tenuto, il Responsabile della protezione dati (DPO)** entro il 28 maggio 2018, data di entrata in operatività del GDPR.

Come noto, il GDPR ha introdotto la figura del DPO, vale a dire il soggetto designato dal titolare o dal responsabile per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR, nonché per fungere da punto di contatto verso l'esterno (Garante privacy) e gli interessati, per le questioni connesse al trattamento dei dati personali.

Il DPO, *che costituisce il fulcro del processo di attuazione del principio di "responsabilizzazione"*, può essere un soggetto interno o esterno all'organizzazione, deve possedere un'approfondita conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, deve agire in piena indipendenza e autonomia e deve poter disporre delle risorse necessarie per l'espletamento dei propri compiti.

L'art. 37 del GDPR prescrive l'obbligo di nominare il DPO, di pubblicare i relativi dati di contatto e di comunicarli al Garante privacy, per:

a) le PA, indipendentemente dai dati oggetto del trattamento. Nel caso in cui soggetti privati esercitino funzioni pubbliche (in qualità, ad esempio, di concessionari di servizi pubblici), il Comitato europeo per la protezione dei dati (EDPB) ha fortemente raccomandato, ancorché non obbligatoria, la designazione del DPO, poiché nei confronti di questi soggetti gli interessati si trovano in una posizione analoga a quella in cui si trovano davanti alla PA in ordine all'*an* e al *quomodo* del trattamento;

b) le imprese private la cui attività principale consista in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) le imprese private la cui attività principale consista in trattamenti su larga scala di dati "sensibili".

Dal provvedimento in esame emerge che **la mancata nomina ovvero la nomina tardiva** - rispetto all'entrata in operatività del GDPR, per i soggetti già obbligati e rispetto al configurarsi dei presupposti, ove successivi - **integra la violazione dell'art. 37, parr 1 e 7,**

[2] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9556625.

del GDPR. Tale violazione, anche alla luce dell'articolata attività informativa rivolta dal Garante privacy ai soggetti chiamati a nominare il DPO, non può considerarsi giustificabile, con conseguente applicazione della sanzione amministrativa pecuniaria.

Nella specie, il Garante ha applicato:

- la sanzione amministrativa pecuniaria di euro 75.000,00 (settantacinquemila);
- la sanzione accessoria della pubblicazione del provvedimento sul sito dell'Autorità.

Si segnala che sulla determinazione delle citate sanzioni ha inciso anche l'accertamento di ulteriori illeciti (assenza della base giuridica e violazione dei principi di "liceità", "limitazione della finalità" e "minimizzazione dei dati").

3. COVID-19. Le FAQ del Garante privacy sul trattamento di dati relativi alla vaccinazione nel contesto lavorativo

Il Garante privacy ha pubblicato sul proprio sito internet le **FAQ sul trattamento di dati relativi alla vaccinazione anti-COVID-19 nel contesto lavorativo**[3]. Le FAQ si aggiungono a quelle pubblicate a maggio dello scorso anno sui trattamenti dei dati personali nel contesto lavorativo nell'ambito dell'emergenza sanitaria.

In particolare, rispetto al trattamento di dati relativi alla vaccinazione anti COVID-19 nel contesto lavorativo, l'Autorità ha affermato che:

1) **il datore di lavoro non può chiedere ai propri dipendenti di fornire informazioni sul proprio stato vaccinale o copia di documenti che attestino l'avvenuta vaccinazione**. L'acquisizione di tali informazioni, infatti, non è consentita né dalle disposizioni dell'emergenza, né dalla disciplina in materia di tutela della salute e sicurezza nei luoghi di lavoro. Essa, inoltre, non può basarsi neppure sul consenso del dipendente, considerato lo squilibrio del rapporto tra titolare (datore di lavoro) e interessato (lavoratore);
2) **il datore di lavoro non può chiedere al medico competente i nominativi dei dipendenti vaccinati**. Solo il medico competente può trattare i dati sanitari dei lavoratori e tra questi, se del caso, le informazioni relative alla vaccinazione, nell'ambito della sorveglianza sanitaria e in sede di verifica dell'idoneità alla mansione specifica (artt. 25, 39, co. 5 e 41, co. 4 del D. Lgs. n. 81/2008). In base al quadro normativo vigente, **il datore di lavoro può acquisire i soli giudizi di idoneità alla mansione specifica** e le eventuali prescrizioni e/o limitazioni in essi riportati (art. 18 co.1, lett. c), g) e bb) del D. Lgs. n. 81/2008). In particolare, secondo il ragionamento del Garante privacy, posta l'assenza di una specifica norma sulla vaccinazione nel contesto lavorativo, la situazione di emergenza *ex se* non può giustificare la conoscenza da parte del datore di lavoro della causa dell'inidoneità alla mansione. In altre parole, ad avviso dell'Autorità, se il legislatore, anche solo a causa dell'emergenza in corso e per la sua durata, non consente al datore di lavoro di acquisire, neppure per il tramite del medico competente,

[3] https://www.garanteprivacy.it/temi/coronavirus/faq#vaccini.

informazioni specifiche in merito alla popolazione dei lavoratori vaccinati, il giudizio di inidoneità rimane per lui ordinariamente "invalicabile" e la conoscenza della causa - vaccinale o meno - della inidoneità continua a restare prerogativa del medico competente;

3) in attesa di un intervento del legislatore nazionale che eventualmente imponga la vaccinazione anti-COVID-19 come requisito per lo svolgimento di determinate professioni, attività lavorative e mansioni, la vaccinazione può costituire solo una misura speciale di protezione nel contesto di attività lavorative con esposizione diretta ad "agenti biologici" *ex* art. 279 del D.Lgs. n. 81/2008 (es. ambito sanitario). Anche in questi casi, solo il medico competente, nella sua funzione di raccordo tra il sistema sanitario e lo specifico contesto lavorativo e nel rispetto delle indicazioni fornite dalle autorità sanitarie anche in merito all'efficacia e all'affidabilità medico-scientifica del vaccino, può trattare i dati personali relativi alla vaccinazione dei dipendenti e, se del caso, tenerne conto in sede di valutazione dell'idoneità alla mansione specifica. Il datore di lavoro deve, quindi, limitarsi ad attuare, sul piano organizzativo, le misure indicate dal medico competente nei casi di giudizio di parziale o temporanea inidoneità.

4. Videosorveglianza. Le FAQ del Garante privacy

Il Garante privacy ha pubblicato sul proprio sito internet le **FAQ in materia di videosorveglianza**[4].

Le FAQ contengono indicazioni di carattere generale in merito al trattamento dei dati personali nell'ambito dell'installazione di impianti di videosorveglianza. Esse fanno seguito all'entrata in operatività del GDPR - alla luce del quale deve essere valutata la validità del provvedimento dello stesso Garante privacy del 2010 - nonché alle Linee guida dell'EDPB in tema di videosorveglianza[5].

Di seguito, le FAQ di maggiore interesse per le imprese:

- **liceità e necessità del trattamento**: l'installazione delle telecamere deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento rilevanti (es. norme in materia di controllo a distanza dei lavoratori). Quanto al profilo della protezione dei dati personali, le modalità di ripresa, la dislocazione delle telecamere e la gestione delle varie fasi del trattamento devono essere improntate al rispetto del principio di minimizzazione, in modo da trattare dati pertinenti e non eccedenti rispetto alle finalità perseguite;
- **autorizzazione**: ai fini dell'installazione delle telecamere non è richiesta alcuna autorizzazione preliminare da parte del Garante privacy;
- **informativa**: gli interessati devono sempre essere informati che stanno per accedere in una zona videosorvegliata. L'informativa, da collocare prima di entrare nella zona

[4] https://www.garanteprivacy.it/faq/videosorveglianza.

[5] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf.

sorvegliata, può essere fornita utilizzando un modello semplificato (anche un semplice cartello), contenente, tra l'altro, le indicazioni sul titolare del trattamento e sulla finalità perseguita. L'informativa deve rinviare a un testo completo contenente tutti gli elementi di cui all'art. 13 del GDPR, indicando come e dove trovarlo (es. sito internet, bacheche, reception);

- **durata della conservazione delle registrazioni**: le immagini registrate non possono essere conservate più a lungo di quanto necessario per le finalità per le quali sono acquisite. In base al principio di responsabilizzazione, spetta al titolare individuare i tempi di conservazione delle immagini, tenuto conto del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione;
- **valutazione d'impatto privacy (DPIA)**: la DPIA è obbligatoria quando il trattamento dei dati - per l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto o le finalità - può presentare un rischio elevato per i diritti e le libertà delle persone. Rispetto all'utilizzo dei sistemi di videosorveglianza, tale rischio può sussistere qualora siano impiegati sistemi integrati - sia pubblici che privati - che collegano telecamere tra soggetti diversi, nonché sistemi intelligenti, capaci di analizzare le immagini ed elaborarle, ad esempio, al fine di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. Inoltre, la DPIA è sempre richiesta, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico e negli altri casi indicati dal Garante (cfr. "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679" dell'11 ottobre 2018);
- **videosorveglianza nelle sedi di lavoro**: l'installazione delle telecamere è consentita esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nel rispetto delle altre garanzie previste dalla normativa di settore in materia di installazione di impianti audiovisivi e altri strumenti di controllo (art. 4 dello Statuto dei lavoratori).

5. Il trattamento dei dati biometrici per finalità di rilevazione della presenza del lavoratore

Con il **provvedimento 14 gennaio 2021, n. 16**[6], il Garante privacy è tornato a pronunciarsi sull'utilizzo dei sistemi di rilevazione delle presenze basati sul trattamento di dati biometrici dei lavoratori (nella specie, le impronte digitali).

Nel provvedimento, l'Autorità ha ricostruito la disciplina applicabile alla fattispecie, soffermandosi, tra l'altro, sul profilo della base giuridica del trattamento dei dati biometrici per finalità di rilevazione della presenza del lavoratore.

[6] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542071.

In particolare, il provvedimento dà atto come, sin dal 2007 e in linea con le pronunce degli altri Garanti privacy Ue, rispetto all'uso dei sistemi biometrici nel contesto lavorativo, il Garante abbia evidenziato la necessità di considerare preventivamente il ricorso ad altri sistemi e/o dispositivi - meno invasivi - che possano assicurare l'attendibile verifica delle presenze, senza fare ricorso al trattamento dei dati biometrici. In tale quadro, a fronte di generiche esigenze di prevenzione circa l'eventuale utilizzo distorto degli strumenti di rilevazione delle presenze d'uso comune (es. i badge), l'Autorità ha valutato **non proporzionato il trattamento dei dati biometrici**, ammettendolo, invece, in limitate ipotesi e in presenza di obiettive e documentate esigenze che rendessero indispensabile l'adozione di tali sistemi, tenuto conto della specificità del caso concreto, del contesto socio-economico di riferimento e delle caratteristiche della tecnologia impiegata (es. provvedimento 15 settembre 2016, n. 357).

Il provvedimento, poi, evidenzia come, a differenza del sistema previgente, il GDPR annoveri i dati biometrici tra le categorie "particolari" di dati personali (ex dati "sensibili") e come tale circostanza impatti *in primis* i presupposti giuridici che rendono leciti i trattamenti di tali categorie di dati, prima ancora che gli aspetti di natura tecnica e le misure di sicurezza.

Infatti, in quanto dati "sensibili", salvo il rispetto dei principi di "liceità, correttezza e trasparenza", "limitazione delle finalità", "minimizzazione", "integrità e riservatezza" dei dati e "responsabilizzazione" (art. 5 del GDPR), i dati biometrici possono essere trattati:

- al ricorrere di una delle condizioni indicate dell'art. 9, par. 2 del GDPR e, in ambito lavorativo, solo quando sia **"necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato**" (art. 9, par. 2, lett. b), del GDPR; art. 88, par. 1 e cons. 51-53 del GDPR);
- nel rispetto di "ulteriori condizioni, comprese limitazioni" (art. 9, par. 4, del GDPR); a tale disposizione è stata data attuazione, nell'ordinamento nazionale, con l'art. 2-*septies* del Codice privacy (come modificato dal D. Lgs n. 101/2018 di adeguamento della normativa nazionale alle disposizioni del GDPR), in base al quale il trattamento dei dati genetici, biometrici e relativi alla salute è lecito al ricorrere di una delle condizioni di cui all'art. 9, par. 2, del GDPR "ed in conformità alle misure di garanzia disposte dal Garante", in relazione a ciascuna categoria dei dati.

Ne consegue che, *in tale quadro, affinché uno specifico trattamento avente a oggetto dati biometrici possa essere lecitamente iniziato è necessario che lo stesso trovi il proprio fondamento in una disposizione normativa che abbia le caratteristiche richieste dalla disciplina di protezione dei dati, anche in termini di proporzionalità dell'intervento regolatorio rispetto alle finalità che si intendono perseguire.*

Infine, il provvedimento sottolinea come, in merito al trattamento dei dati biometrici, il difetto di base giuridica **non possa essere superato né dal consenso** dei dipendenti, posto che esso non costituisce, di regola, un valido presupposto di liceità per il trattamento dei dati personali in ambito lavorativo, **né richiamando il legittimo interesse del titolare**, in quanto, lo stesso non è applicabile al trattamento di categorie particolari di dati personali.

6. Brexit

Dal 1° gennaio 2021 il Regno Unito ha lasciato definitivamente l'Unione europea, diventando dunque un Paese terzo.

Per quanto riguarda i flussi di dati verso il Regno Unito, si segnala che il 30 dicembre scorso, il Regno Unito e l'Unione europea hanno stipulato un **Accordo commerciale e di cooperazione**[7], in base al quale, tra l'altro, il Regno Unito continua ad applicare il GDPR fino al 30 giugno 2021. Pertanto, fino a tale data, qualsiasi comunicazione di dati personali verso il Regno Unito potrà avvenire non sarà considerata un trasferimento di dati verso un Paese terzo e potrà svolgersi secondo le medesime regole applicate al 31 dicembre 2020.

Intanto, al fine di far proseguire i flussi di dati senza interruzioni anche successivamente al 30 giugno p.v., la Commissione europea ha adottato **una proposta di decisione di adeguatezza**[8] in merito ai flussi di dati UE-Regno Unito.

Secondo quanto dichiarato durante la presentazione della proposta, la Commissione europea ha valutato attentamente il diritto e la prassi del Regno Unito in materia di protezione dei dati personali, comprese le norme sull'accesso ai dati da parte delle autorità pubbliche. Ha, dunque, concluso che il Regno Unito assicura un livello di protezione essenzialmente equivalente a quello garantito dal GDPR.

La decisione dovrebbe essere efficace per un periodo di 4 anni, alla scadenza dei quali verrebbe soggetta a un riesame.

Quanto all'*iter*, la proposta è all'esame dell'EDPB per il parare e dovrà essere approvata da un comitato composto da rappresentanti degli Stati membri.

[7] https://ec.europa.eu/info/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en.

[8] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.