STEFANELLI & STEFANELLI STUDIO LEGALE

IL MIO DPO

rivista di aggiornamento sugli adempimenti privacy

a cura del team privacy Studio Legale Stefanelli & Stefanelli

Pubblicazione nr. 1 /2021
marzo 2021

Pubblicazione di Stefanelli & Stefanelli servizi legali s.r.l.s.
Via Azzo Gardino 8/A - 40122 Bologna
info@stefanelli-servizilegali.it

PREFAZIONE

La normativa in materia di trattamento dei dati personali si arricchisce ogni giorno dei provvedimenti attuativi dei garanti nazionali, delle decisioni di natura sanzionatoria, delle Linee guida dell'European Data Protection Board (EDPB), delle sentenze dei giudici nazionali e della Corte di giustizia europea.

Il corretto trattamento dei dati personali passa dunque non solo attraverso la conoscenza del Regolamento (UE) 2016/679 e del Codice Privacy, ma anche attraverso la conoscenza e lo studio del ricchissimo e prezioso materiale prodotto ogni giorno dalle autorità competenti e dai giudici su tutto il territorio nazionale e comunitario.

Lo Studio Legale Stefanelli&Stefanelli ha deciso quindi di selezionare e raccogliere i contenuti di cui ritiene imprescindibile la conoscenza da parte dei Titolari e Responsabili del trattamento, mettendoli a disposizione delle organizzazioni che hanno scelto di affidarci il ruolo di DPO con un breve focus su ciascuna novità e un approfondimento redatto dai nostri esperti della materia, allo scopo di fornire a coloro che devono gestire e organizzare il trattamento dei dati personali una modalità di aggiornamento rapida ed efficace.

Studio Legale Stefanelli & Stefanelli

INDICE DEI CONTENUTI

INDICE DEI CONTENUTI

INDICE DEI CONTENUTI

INDICE DEI CONTENUTI

Sanzione al Ministero dello sviluppo Economico per non aver nominato il DPO

Tra le lezioni che il Garante italiano sta cercando di dare è che dall'applicazione del GDPR nessuno può dirsi esente!

Lo fa, questa volta, in merito all'applicazione dell'articolo 37 del GDPR in tema di Data Protection Officer nel provvedimento n. 54/2021.

In particolare, il Garante privacy ha emesso un'ordinanza di ingiunzione del valore di 75.000,00 € nei confronti del M.I.S.E. (Ministero dello Sviluppo Economico) 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 e per avere diffuso sul sito web istituzionale informazioni personali di oltre 5.000 manager.

La mancata nomina è stata scoperta durante l'istruttoria avviata in seguito alle segnalazioni ricevute dal Garante sulla presenza di un elenco di manager sul sito web del MiSE. Questo elenco conteneva numerosi dati personali di oltre 5.000 professionisti: nome, codice fiscale, indirizzi email e il curriculum vitae completo con ulteriori dati, tra cui numero di telefono, istruzione e formazione, esperienze professionali, documento di riconoscimento e tessera sanitaria.

L'autorità ha rilevato un **trattamento di dati personali sproporzionato** e quindi **non conforme** alla normativa in vigore.

Il Garante spiega che il MiSE doveva utilizzare strumenti meno invasivi per la divulgazione dei dati, evitando il rischio di usi illegittimi da parte di terzi (furto d'identità, profilazione, phishing e altro).

Ma oltre a tale infrazione, il Garante si accerta dell'assenza del DPO.

È la prima volta che 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 del Regolamento.

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) ed è la prima volta che il Garante privacy, peraltro incidentalmente, prende provvedimenti in tal senso.

Garante Italiano - Ordinanza di ingiunzione nei confronti di Ministero dello Sviluppo Economico - 11 febbraio 2021 [Doc. Web 9556625]

Vai all'Ordinanza

Diritto di accesso: scheda informativa del Garante

Il Garante ha pubblicato delle **schede sui diritti di accesso**, con cui vengono affrontati per punti e con un linguaggio semplice il tema del diritto di accesso, analizzando sia il caso generale DIRITTO DI ACCESSO DELL'INTERESSATO sia alcuni casi particolari come

- DIRITTO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI
- DIRITTO DI ACCESSO RIGUARDANTE PERSONE DECEDUTE
- DIRITTO DI ACCESSO CIVICO SEMPLICE E GENERALIZZATO

Garante Italiano - Le schede sui diritti di accesso ai dati personali

Vai al sito del Garante per scaricare le schede

Italia: Regione Lazio riceve sanzione di 75.000 euro per non aver nominato un responsabile del trattamento

Regione Lazio è stata sanzionata dal Garante per un totale di 75.000 euro per non aver nominato come responsabile del trattamento la cooperativa che gestiva il call center del CUP e quindi le prenotazioni delle prestazioni sanitarie, trattando di fatto i dati illecitamente dal 1999 al 2019

La cooperativa stessa aveva fatto più volte presente a Regione Lazio, Titolare del trattamento, la necessità della propria nomina a responsabile, inoltre aveva messo in atto le proprie misure di sicurezza in conformità al GDPR: ha pertanto ricevuto solo un'ammonizione dal Garante.

Italia: il Garante sanziona l'Inps per 300mila euro per le modalità dei controlli per il bonus Covid

Il Garante ha emesso una sanzione di 300.000,00 euro nei confronti dell'INPS, per le modalità utilizzate nell'effettuare i controlli per i richiedenti del c.d. "Bonus Covid".

L'Autorità ha rilevato una mancata definizione dei criteri per trattare i dati di determinate categorie di richiedenti, l'uso di informazioni non necessarie rispetto alle finalità di controllo, ricorso a dati non corretti o incompleti, inadeguata valutazione dei rischi per la privacy.

L'istruttoria ha messo in luce che l'INPS non aveva adeguatamente progettato il trattamento e non è stata in grado di dimostrare di aver svolto i controlli nel rispetto del GDPR, violando così i principi di privacy by design, privacy by default e accountability.

Linee Guida EDPB su esempi di notifica data breach

L'European Data Protection Board (EDPB) ha pubblicato le **"Linee guida 01/2021 sugli esempi riguardanti la notifica della violazione dei dati"** con l'obiettivo di assistere i titolari del trattamento nella gestione delle violazioni di dati personali.

L'EDPB ha optato per un taglio molto pratico ed ha fornito molteplici esempi di violazione di dati personali: per ciascuna categoria di violazione dei dati, vengono fornite indicazioni per valutare il livello di rischio connesso alla specifica violazione di dati, sulla base delle circostanze della violazione medesima e della natura del trattamento di dati coinvolto.

Così, l'EDPB fornisce un duplice aiuto:

- In primo luogo, per comprendere **se una specifica violazione dei dati debba essere notificata** all'Autorità Garante e eventualmente comunicata agli interessati;
- In secondo luogo, sulle **misure di sicurezza** che i Titolari possono adottare per **arginare i rischi** connessi alla violazione medesima.

L'EDPB ha voluto porre particolare attenzione sulle misure tecniche e organizzative che i Titolari adottano presso la propria organizzazione, sottolineando come il rispetto del criterio dell'adeguatezza talvolta può quasi del tutto annullare il rischio derivante dalla violazione di dati verificatasi presso la struttura del Titolare.

E.D.P.B. European Data Protection Board - Guidelines 01/2021 on Examples regarding Data Breach Notification

Vai al sito EDPB

Autovalutazione per la notifica del data breach

Il Garante per la Protezione dei dati personali ha messo a disposizione dei titolari del trattamento uno **strumento di autovalutazione dei data breach** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza

Lo strumento si basa su un sistema progressivo di domande che sono corredate da esempi ed indicazioni utili a guidare l'utente nel fornire le giuste risposte.

A form completato, l'utente riceve indicazioni circa

- la **necessità di procedere alla notifica del data breach** all'Autorità Garante;
- la necessità di procedere con la **comunicazione** del data breach anche **agli interessati.**

Garante Italiano - Autovalutazione per individuare le azioni da intraprendere a seguito di una violazione dei dati personali

Vai al sito del Garante per accedere allo strumento di autovalutazione

Italia: sanzione di €8.000 del Garante per furto di un hard disk esterno

Il Garante Italiano ha sanzionato l'Agenzia regionale protezione ambientale Campania (ARPAC) per **inadeguatezza delle misure tecniche e organizzative** per garantire la sicurezza dei trattamenti in occasione di un data breach.

In particolare, il caso riguarda il **furto di un dispositivo** (nel caso un hard disk, ma sarebbe potuto essere una chiavetta USB) contenente dati, notificato come data breach al Garante italiano.

Il furto, avvenuto presso i locali della U.O.C. Siti contaminati e Bonifiche dell'Agenzia, ha per oggetto un hard disk esterno contenente dati personali quali copie di documenti di riconoscimento, documenti fiscali, un elenco di dati analitici di procedimenti giudiziari e molto altro.

Segnalo di seguito i punti – a mio avviso - meritevoli di attenzione:

1. non viene escluso che il data breach sia stato doloso e che abbia comportato una possibile divulgazione non autorizzata dei dati: di conseguenza determina un rischio per le libertà e i diritti degli interessati;
2. **tale violazione ha compromesso riservatezza e disponibilità dei dati**, inoltre, dalla documentazione fornita, risulta anche che non erano state adottati accorgimenti necessari a consentire la continuità, su base permanente, e il ripristino della disponibilità dei dati personali sottratti, nonché irreparabilmente persi;
3. l'hard disk oggetto di furto sarebbe stato collegato a un server situato in una stanza a cui qualsiasi dipendente poteva accedere: ad aggravare la situazione sarebbe stato il fatto che all'interno del dispositivo erano stati impropriamente memorizzati dati riguardanti i familiari dei dipendenti. Tutti i soggetti coinvolti, però, sono stati contattati in merito all'avvenuto furto e sono stati esortati ad attivare ogni eventuale precauzione per proteggersi da potenziali conseguenze negative. In conclusione, al fine di mitigare ulteriori episodi simili, l'ARPAC ha adottato ulteriori misure di sicurezza fisiche.

L'ARPAC ha dimostrato piena collaborazione nei confronti del Garante, fornendogli elementi per la ricostruzione dell'accaduto come l'auto dichiarazione dei dipendenti circa la memorizzazione dei propri dati e le copie di alcuni dei documenti contenuti nell'Hard Disk come prova che gli stessi non contengono dati personali relativi a condanne penali.

L'ARPAC per il Garante si è resa responsabile della violazione degli artt. 5, par. 1, lett. f), e 32 del GDPR.

La sanzione applicata è stata di **8.000 euro, ammontare che ha tenuto conto della tipologia e quantità dei dati, non risultando compromessi informazioni rientranti nella categoria di dati particolari o relativi a condanne penali e reati.**

Indubbiamente anche l'atteggiamento collaborativo del Titolare ha inciso sulla quantificazione della sanzione.

In tutte le aziende, l'attenzione ai dispositivi esterni deve essere un elemento su cui riflettere perché potrebbe essere facilmente oggetto di breach.

Germania: Autorità della Bassa Sassonia multa un'azienda per 10,4 milioni di euro per videosorveglianza illecita

Una società di e-commerce tedesca monitorava illecitamente i propri dipendenti attraverso un sistema di videosorveglianza che aveva telecamere installate in vari locali aziendali, tra cui le sale di vendita, i magazzini e le aree comuni.

Il caso arriva avanti al Garante della Bassa Sassonia che ha inflitto una multa di ben 10,4 milioni di euro.

La società sanzionata si è giustificata affermando che lo scopo delle telecamere installate era quello di prevenire e indagare sui reati e di tracciare il flusso delle merci nei magazzini, ma come sottolinea l'autorità tedesca **per prevenire i furti le aziende non possono ricorrere ad una videosorveglianza indiscriminata negli ambienti di lavoro**.

Viceversa **in presenza di un sospetto devono agire gradualmente** con controlli inizialmente meno invasivi, come possono essere quelli effettuati a campione sui bagagli di chi esce dai locali commerciali.

Non solo.

La videosorveglianza per scoprire i reati è lecita solo se esiste un fondato sospetto nei confronti di determinate persone.

Mentre nel caso esaminato il funzionamento delle telecamere non era né limitato a un determinato periodo né a dipendenti specifici, e in molti casi le registrazioni venivano salvate per 60 giorni, un tempo notevolmente più lungo del necessario.

Gli interessati sorvegliati in modo sproporzionato erano sia i dipendenti che i clienti o potenziali clienti.

Un caso di videosorveglianza illecita, quindi, in quanto utilizzata i modo sproporzionato e lesiva dei diritti soprattutto dei dipendenti, impossibilitati a opporsi a tale trattamento indiscriminato.

Infine, come ha precisato il Garante, potevano essere utilizzati altri modi per prevenire furti all'interno dei locali.

Spagna: sanzione di € 6.000.000 per trattamento illecito e informazioni insufficienti

L'Autorità Garante spagnola (AEPD) ha ritenuto illecito il trattamento di dati personali di CAIXABANK per **carenza delle informazioni** relative alle categorie di dati personali trattati, alle finalità e alla base giuridica del trattamento, con particolare riguardo ai trattamenti basati sul legittimo interesse dell'azienda.

Di conseguenza, ha inflitto una **sanzione di € 2.000.000** alla banca per violazione degli artt. 13 e 14 del GDPR. L'AEPD ha inoltre rilevato che CAIXABANK **non prevedeva alcun meccanismo di raccolta del consenso dell'interessato** e che, in ogni caso, tale consenso non poteva considerarsi valido. Inoltre ha ritenuto che le attività di trattamento basate sul legittimo interesse dell'azienda non erano sufficientemente giustificate, infliggendo pertanto un'ulteriore sanzione di €4.000.000 per violazione dell'art. 6 del GDPR.

Norvegia: l'Autorità intende multare Grindr per una somma di 10 milioni di euro

L'Autorità norvegese per la protezione dei dati (Datatilsynet) ha inviato a Grindr LLC una "advance notification" in cui viene espressa l'intenzione di emettere una sanzione amministrativa di NOK 100000000 (circa **10 milioni di euro**) per il **mancato rispetto delle norme del GDPR** sul consenso (10% fatturato annuo).

Grindr è un social per persone gay, bisessuali, trans e queer con 13,7 milioni di utenti attivi.

Le violazioni rilevate dall'Autorità riguardano il fatto che gli utenti sono stati costretti ad accettare l'informativa sulla privacy nella sua interezza per poter utilizzare l'app, non predisponendo una richiesta di consenso specifica per la condivisione dei propri dati (anche relativi alle preferenze sessuali) con terze parti per fini di marketing, e non fornendo agli utenti informazioni sufficienti sulla condivisione dei propri dati personali.

Trasferire i dati verso Paesi Extra UE dopo SCHREMS II. Come si stanno muovendo le autorità europee

Le Autorità europee, a seguito delle incertezze causate dalla Sentenza Schrems II sul trasferimento dei dati extra-UE, sono intervenute con:

Le Raccomandazioni 02/2020 dell'EDPB

L'11 novembre 2020, l'European Data Protection Board ha adottato le raccomandazioni sulle misure per il trasferimento dei dati verso paesi terzi.

Secondo l'Autorità, in questi casi, i titolari del trattamento che utilizzano clausole contrattuali standard (SCC) devono controllare se le legislazioni del paese terzo garantiscano un adeguato livello di protezione dei dati personali trasferiti equivalente a quello dello Spazio Economico Europeo.

Sul tema, poi, la Corte di Giustizia dell'Unione europea ha previsto la possibilità di aggiungere delle misure cautelative supplementari alle clausole contrattuali standard, per agevolare i Titolari del trattamento a trasferire i dati personali verso paesi terzi, nel caso in cui le clausole contrattuali standard non siano sufficienti.

Le nuove Clausole Contrattuali Standard (SCC)

In aggiunta, la Commissione Europea ha sottoposto a consultazione pubblica le nuove clausole contrattuali standard (SCC) sul trasferimento di dati personali extra UE con l'intento di cambiare il clima di incertezza sull'effettiva applicabilità delle attuali SCC.

Per approfondimenti si rimanda all'articolo
"Trasferire dati verso paesi extra-EU dopo la Schrems II: come si stanno muovendo le Autorità europee"
a cura dell'Avv. Vittoria Piretti

Il nuovo modello di clausole contrattuali standard

Il 12 novembre 2020 la Commissione europea ha pubblicato la **bozza delle nuove Calusole Contrattuali Standard (SCC).**

Quali novità?

Le SCC non prevedono più la dicotomia:

- titolare à titolare
- titolare à responsabile

Saranno invece previsti 4 moduli:

- titolare à titolare
- titolare à responsabile
- responsabile à reaponsabile
- responsabileà sub-responsabile

Il nuovo documento allinea il nuovo modello di Standarc Contractual Clauses al GDPR.

Esso si propone di disciplinare meglio i "trasferimenti più complessi" che vedono coinvolti più esportatori e/o più importatori.

La finalizzazione del documento è prevista per questa primavera.

E.D.P.B. European Data Protection Board - Notizie: "Il comitato europeo per la protezione dei dati e il Garante europeo per la protezione dei dati adottano pareri congiunti su nuove clausole contrattuali tipo"

Vai al sito EDPB per leggere la notizia completa

Brexit: quale sorte per il trasferimento dei dati personali in UK nel 2021

Secondo il Trade and Cooperation Agreement (Accordo di Cooperazione e Commercio), **l'UE e l'UK devono impegnarsi a garantire i flussi transfrontalieri di dati, al fine di agevolare gli scambi nell'economia digitale**, nonché a mantenere alti i livelli di protezione dei dati.

I trasferimenti dei dati personali tra UE e UK saranno regolati da decisioni di adeguatezza, prese unilateralmente da ciascun Paese. Tuttavia, la Commissione europea sta ancora lavorando su tali decisioni di adeguatezza.

Si pone, dunque, il problema della regolamentazione del flusso di dati personali tra UE e UK in pendenza dell'adozione delle decisioni di adeguatezza.

Il Trade and Cooperation Agreement ha previsto tale problematica e, a partire dal 1 gennaio 2021, considera applicabile la c.d. *bridging clause* (clausola ponte).

Quest'ultima consente il libero flusso di dati personali dalla UE a UK per un periodo massimo di 6 mesi, con alcune specifiche restrizioni.

Per approfondimenti si rimanda all'articolo
"Brexit: quale sorte per i trasferimenti di dati personali in UK nel 2021?"
a cura dell' Avv. Maria Livia Rizzo

GDPR e Brexit: verso una regolamentazione dei flussi di dati verso il Regno Unito

Nel febbraio 2021 la Commissione europea ha avviato il processo di adozione di due decisioni di adeguatezza per i trasferimenti di dati personali nel Regno Unito post-Brexit, una ai sensi del Regolamento generale sulla protezione dei dati e l'altra per la Direttiva (UE) 2016/680.

La decisione di adeguatezza adottata dalla Commissione ha l'obiettivo di attestare che un determinato paese terzo garantisce un livello di protezione dei dati personali equivalente a quello previsto all'interno dell'UE. Qualora la Commissione adotti tale decisione, sarà possibile trasferire i dati personali dall'Ue a quel determinato paese terzo.

Nel caso del Regno Unito, dunque, sarà la decisione di adeguatezza a fungere da fondamento per un lecito trasferimento dei dati dall'Unione europea a tale paese. Il governo del Regno Unito ha indicato che intende accettare la decisione di adeguatezza della Commissione europea prima della fine del periodo di transizione (dal 1 gennaio 2021 al 30 giugno 2021), garantendo la continua libera circolazione dei dati.

Per approfondimenti si rimanda all'articolo
"GDPR e Brexit: verso una regolamentazione dei flussi di dati verso il Regno Unito"
a cura dell' Avv. Alessandra Delli Ponti

Linee Guida 09/2020 in materia di obiezione rilevante e motivata ai sensi del Regolamento 2016/679

In data 8 ottobre 2020, l'European Data Protection Board (di seguito anche EDPB) ha adottato le Linee Guida sul concetto di "**obiezione pertinente e motivata**" contenuto all'interno del GDPR (art. 4, n. 24).

L'Autorità è intervenuta per chiarire quando, nell'ambito di un **trattamento di dati transfrontaliero** (e dunque che interessa più Paesi), **la decisione di violazione del GDPR adottata dall'Autorità capofila** (ossia l'autorità che ha sede nel luogo del principale stabilimento del Titolare del trattamento) **possa essere contestata dalle altre Autorità di controllo interessate**.

Secondo l'EDPB il concetto di "obiezione pertinente e motivata" funge da "soglia" in tali situazioni, ciò significa che **l'obiezione delle Autorità interessate avverso l'operato dell'Autorità capofila può essere presentata esclusivamente qualora sia effettivamente pertinente e motivata.**

L'EDPB ritiene tale l'obiezione se essa indica ogni parte del progetto di decisione che è considerata carente, errata o priva di alcuni elementi necessari, facendo riferimento a specifici articoli/paragrafi, e mostrando perché tali questioni sono da considerarsi "rilevanti".

Pertanto, l'obiezione deve mirare, in primo luogo, ad evidenziare come e perché il progetto di decisione non affronta adeguatamente la situazione di violazione del GDPR e/o non prevede un'azione appropriata nei confronti del Titolare del trattamento. Infine, le proposte di modifica avanzate dall'obiezione dovrebbero mirare a rimediare a questi errori.

E.D.P.B. European Data Protection Board - Guidelines 09/2021 on relevant and reasoned objection under Regulation 2016/679

Vai al sito EDPB

Rapporto Clusit sugli eventi di cyber-crime più significativi avvenuti a livello globale nel 2020

È stato pubblicato il **rapporto dell'Associazione Italiana per la Sicurezza Informatica (CLUSIT) relativo agli eventi di cyber-crime più significativi** nel mondo dell'ultimo anno.

Quanto emerge è che **nel corso del 2020 gli attacchi informatici sono aumentati del 12% rispetto al 2019**.

Il 2020 si inserisce quindi a pieno titolo in un trend di crescita costante del cybercrime che, dal 2017, è aumentato del 66%.

Per quanto riguarda in particolare il settore della sanità, questa è stata oggetto del 12% degli attacchi informatici totali del 2020.

All'interno del report è possibile vedere il numero totale degli attacchi classificati secondo alcuni criteri, tra cui ad esempio il tipo di malware utilizzato o gli obiettivi colpiti dai cyber-criminali.

CLUSIT - Associazione Italiana per la Sicurezza Informatica - Rapporto Clusit 2021

Vai al sito del Clusit

Italia: come il crash dei dati di un server può far chiudere un'azienda

Vintag, un'app bolognese per vendere abiti e oggetti vintage online, **era tra le start up italiane più promettenti nel mondo della moda**, finché con il **crash dei server** di un'azienda esterna non ha perso tutti i dati accumulati in 5 anni di attività.

Per la maggior parte delle aziende i dati aziendali e sulle preferenze di consumo degli utenti sono tutto, e per questo **Vintag è stata costretta a chiudere**.

La struttura sanitaria può consentire l'accesso alle cartelle cliniche del defunto?

L'approfondimento ha l'obiettivo di assistere le strutture sanitarie che ricevono **richieste di accesso alla cartella clinica dei defunti.**

Può infatti avvenire che, in seguito alla morte di una persona, un suo erede legittimo che è stato escluso dalla successione manifesti l'interesse ad impugnare il testamento sulla base di una ritenuta incapacità del defunto a disporre del proprio patrimonio ex art. 591 del Codice Civile.

L'articolo fornisce i chiarimenti necessari a verificare se un determinato soggetto sia legittimato a esercitare il diritto di accesso alla documentazione sanitaria, al fine di tutelare un proprio diritto in sede giudiziaria.

Per approfondimenti si rimanda all'articolo
"Può la struttura sanitaria consentire l'accesso alle cartelle cliniche dei defunti?"
a cura dell' Avv. Maria Livia Rizzo, Dott.ssa Federica Pucarelli

Garante Italiano - Scheda Diritti riguardanti persone decedute

Consulta la pagina di riferimento

Opposizione al Fascicolo Sanitario Elettronico. Il Garante interviene confermando che non esiste alcun termine.

A seguito della diffusione di notizie relative all'esistenza di un **presunto termine per l'opposizione alla costituzione del Fascicolo Sanitario Elettronico**, molteplici strutture sanitarie hanno ricevuto una moltitudine di richieste in tal senso da parte dei cittadini.

Il Garante è intervenuto sul punto precisando che:

- A partire da maggio 2020, **senza il consenso degli interessati**, i dati di tutte le prestazioni sanitarie fruite confluiscono **automaticamente** nel Fascicolo sanitario elettronico (ovviamente, per le sole Regioni che hanno attivato il FSE);
- In ogni caso, i dati sanitari dei cittadini \ in assenza di uno specifico consenso del singolo cittadino;
- i dati delle prestazioni sanitarie effettuate prima del maggio 2020, potranno confluire nel FSE solo a tre condizioni:
    1. idonea campagna nazionale di informazione;
    2. informazione ai cittadini delle Regioni interessate sulle novità relative all'alimentazione del Fascicolo;
    3. riconoscimento di un termine non inferiore a 30 giorni per manifestare la propria eventuale opposizione.

Allo stato di fatto, non essendosi verificata nessuna di queste condizioni, **l'esercizio del diritto di opposizione all'alimentazione del FSE è priva di ogni fondamento giuridico**.

Garante Italiano - Fascicolo sanitario elettronico: nessuna scadenza per l'inserimento dei dati

Comunicato Stampa

Sanzione alla Fondazione di religione e di culto "Casa sollievo della sofferenza" Opera di San Pio da Pietrelcina

La Fondazione di religione e di culto "Casa sollievo della sofferenza" Opera di San Pio da Pietrelcina è stata sanzionata dal Garante per 5.000,00 euro per la violazione del principio di esattezza dei dati che ha comportato l'erronea trasmissione, a mezzo di posta tradizionale, di documentazione sanitaria a un soggetto terzo non autorizzato per un caso di omonimia.

La fattura, emessa dalla Fondazione per le spese di invio del plico postale, è stata erroneamente attribuita ad altro interessato omonimo (dati errati: indirizzo di residenza).

Tali dati (errati) sono stati utilizzati successivamente per la composizione del plico di spedizione, a mezzo posta, del referto sanitario relativo al reale interessato.

L'operatore addetto alla composizione del plico postale non ha verificato la corrispondenza dei dati anagrafici presenti in fattura con quelli presenti sul referto sanitario, dati identici per cognome e nome e differenti tra loro solo per l'indirizzo di residenza.

Garante Italiano - Ordinanza ingiunzione nei confronti di Fondazione di religione e di culto "Casa sollievo della sofferenza" Opera di San Pio da Pietrelcina - 11 febbraio 2021 [Doc Web. 9567489]

Vedi il provvedimento

Sanzione ASL2 Abruzzo Vasto Lanciano Chieti

L'Azienda Sanitaria Locale n. 2 Lanciano-Vasto-Chieti è stata sanzionata (6.500 euro) per la spedizione, in formato cartaceo, di documentazione, contenente referti relativi ad esami ematici di un bambino, a un soggetto diverso da quello legittimato a riceverla per un **errore umano nell'imbustamento**.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Sanitaria Locale n. 2 Lanciano-Vasto-Chieti - 11 febbraio 2021 [Doc Web9567143]

Vedi il provvedimento

Sanzione AUSL Toscana Locale Sud Est

Con Provvedimento n. 278 del 17 dicembre 2020, il Garante Privacy ha comminato una **sanzione di € 100.000 a una Azienda USL** per illecito trattamento di dati personali.

La peculiarità risiede nel fatto che il "trattamento sanzionato" era stato **avviato a cavallo tra la vecchia e la nuova normativa**.

L'articolo si pone quindi l'obiettivo di fornire indicazioni su come rivalutare, adeguare e monitorare tutti quei trattamenti iniziati in epoca pre-GDPR e ancora in corso.

Per approfondimenti si rimanda all'articolo
"Ausl sanzionata per 100.000 € per illecito trattamento di dati personali. Cosa ci insegna questo provvedimento?"
a cura dell'Avv. Maria Livia Rizzo, Dott.ssa Federica Pucarelli

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Unità Sanitaria Locale Toscana Sud Est - 17 dicembre 2020 [Doc Web 9529527]

Vedi il provvedimento

Sanzione AOU Parma

L'Azienda Ospedaliero Universitaria di Parma ha ricevuto una s**anzione di 10.000 euro** per aver **erroneamente consegnato** a un erede di un paziente defunto di **una cartella clinica** contente un referto contenente gli esami ematochimici di un altro paziente.

L'AOU aveva inviato notifica di data breach al Garante e chiesto al ricevente la riconsegna della copia della cartella clinica: a fronte di un atteggiamento non collaborativo ha proceduto a richiedere formalmente la restituzione del documento, diffidandolo dall'utilizzarne i dati, e a compiere un'autovalutazione delle modalità di gestione delle cartelle cliniche.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Ospedaliero Universitaria di Parma - 27 gennaio 2021 [Doc Web 9544092]

Vedi il provvedimento

Sanzione AOU Senese

A causa di un **errore materiale in fase di imbustamento, soggetti terzi ricevevano** per posta presso la loro residenza **una relazione medica cartacea riferita ad altri soggetti interessati**.

Il documento cartaceo veniva recuperato e l'L'Azienda Ospedaliero Universitaria metteva in atto misure organizzative atte ad evitare il ripetersi dell'errore, come

- lo spostamento fisico dell'operatore addetto alle operazioni di imbustamento e spedizione delle relazioni mediche in ambiente più idonee e
- l'adozione di un indirizzo PEC per l'invio in sostituzione del metodo cartaceo.

Il Garante ha ritenuto pertanto che non fossero necessarie misure correttive ai sensi dell'art. 58 par. 2 del Regolamento, erogando però la sanzione di € 10.000 per violazione dei principi del trattamento.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Ospedaliero Universitaria Senese - 27 gennaio 2021 [Doc Web9544457]

Vedi il provvedimento

Sanzione Azienda Ospedaliera Regionale "San Carlo" di Potenza

L'Azienda ospedaliera regionale "San Carlo" di Potenza ha riceva s**anzione di 70.000 euro per aver diffuso** tramite la diramazione di un comunicato stampa **informazioni numerose e dettagliate sullo stato di salute di un paziente e sulle terapie intraprese**, successivamente al suo decesso per Covid-19.

Il Garante ha infatti ritenuto che la finalità di informare la popolazione in merito alle cure offerte dall'Azienda ai pazienti Covid-19 poteva essere raggiunta anche senza diffondere informazioni cliniche di dettaglio sul paziente.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda ospedaliera regionale "San Carlo" di Potenza - 27 gennaio 2021 [Doc Web 9549143]

Vedi il provvedimento

Sanzione AUSL Bologna

L'Azienda Sanitaria Locale di Bologna ha ricevuto **18.000 euro di sanzione** per **l'erroneo inserimento di documenti sanitari in 182 Fascicoli Sanitari Elettronici**, di cui 49 erano attivi.

L'incidente, notificato al Garante, sarebbe stato generato da un errore manuale di un tecnico appartenente a una ditta terza e, dopo circa 6 ore dalle segnalazioni dei pazienti, i documenti erroneamente inseriti sono stati cancellati.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Usl di Bologna - 14 gennaio 2021 [Doc Web 9542155]

Vedi il provvedimento

Sanzione AO San Pio Benevento

L'Azienda Ospedaliera pubblicava sulla propria rete intranet, accessibile a tutti i dipendenti tramite username e password, dati ed informazioni personali contenuti nella graduatoria finale relativa all'attribuzione delle progressioni economiche orizzontali riferiti a circa **750 dipendenti e le relative schede di valutazione**; oltre i dati identificativi venivano pubblicati anche informazioni sull'anzianità di servizio, le esperienze professionali e l'indicazione dei punteggi.

L'Azienda Ospedaliera giustificava la decisione sulla base di un accordo sindacale e sulla necessità di concludere velocemente la procedura e permettere ai dipendenti l'accesso agli atti ex l. n. 241/90.

Il Garante ha ritenuto che per la finalità dichiarata, ovvero garantire l'accesso agli atti, la pubblicazione sulla intranet aziendale non sia conforme al requisito della protezione dei dati fin dalla progettazione ovvero al rispetto del principio di privacy by default e by design.

Il Garante ha quindi ritenuto di erogare la sanzione amministrativa, modulando però l'importo sulla base dei criteri previsti dall'art. 83, par. 2 ovvero ha tenuto conto del fatto che:

- la comunicazione è avvenuta nei confronti di soggetti determinati muniti di credenziali
- i dati trattati non appartenevano a categorie particolari
- la pubblicazione è stata limitata nel tempo
- la condotta è stata determinata da un'errata valutazione delle modalità di attuazione dell'accordo sindacale
- l'amministrazione ha collaborato con l'Autorità Garante.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Ospedaliera San Pio di Benevento - 14 gennaio 2021 [Doc Web 9543138]

Vedi il provvedimento

Sanzione Poliambulatorio Talenti srl

Il Garante Privacy ha **sanzionato per un importo di € 2.000** il Poliambulatorio Talenti S.r.l. per non aver dato riscontro alla richiesta d'accesso dell'interessato entro 30 giorni (ex art. 15 GDPR), se non dopo ulteriore reclamo dell'interessato e invito del Garante a fornire riscontro.

Garante Italiano - Ordinanza ingiunzione nei confronti di Poliambulatorio Talenti S.r.l. - 14 gennaio 2021 [Doc Web 9542096]

Vedi il provvedimento

Sanzione ASP Enna

L'Autorità Garante ha comminato una **sanzione da 30.000 euro** all'Azienda Sanitaria Provinciale di Enna per le **rilevazioni e il trattamento dei dati delle impronte digitali per rilevare la presenza dei dipendenti e scoraggiare il fenomeno dell'assenteismo**.

Il Garante ha ritenuto che il trattamento fosse sproporzionato rispetto alle finalità, privo di una base giuridica adeguata e che inoltre ai dipendenti non fosse stata fornita informativa chiara e completa.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Sanitaria Provinciale di Enna - 14 gennaio 2021 [Doc Web 9542071]

Vedi il provvedimento

Sanzione AUSL Toscana Centro

Il Garante italiano ha **sanzionato** l'ASL Toscana Centro per un totale di **10.000 euro**, in seguito a istruttoria conseguente a una segnalazione.

Il segnalante lamentava infatti le modalità con le quali i pazienti erano chiamati a depositare il campione biologico per la prevenzione dei tumori intestini in un frigo deputato alla custodia degli stessi e la relativa modulistica compilata dai partecipanti, lamentando **l'assenza di personale addetto alla custodia dei predetti reperti e dei documenti.**

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda Unità Sanitaria Locale Toscana Centro - 6 febbraio 2020 [Doc Web 9299150]

Vedi il provvedimento

Sanzione AUSL Romagna

Il Garante italiano ha **sanzionato** l'Azienda USL della Romagna per **50.000 euro per erronea comunicazione di dati a soggetto non autorizzato**, dovuta a errata verifica dell'anagrafica di una paziente.

Nonostante l'adozione di misure tecniche ed organizzative a protezione dei dati personali e soprattutto l'attuazione di un nuovo sistema di gestione delle anagrafiche volto ad evitare altre violazioni di dati simili a quella verificatasi, il Garante ha comunque ritenuto di comminare la sanzione.

Garante Italiano - Ordinanza ingiunzione nei confronti di Azienda USL della Romagna - 27 gennaio 2021 [Doc Web 9544504]

Vedi il provvedimento

Olanda: sanzione di 440.000 euro a ospedale per inadeguata protezione delle cartelle cliniche

L'Autorità olandese ha avviato le indagini a seguito di segnalazioni sui media e a seguito di due notifiche di violazioni di dati relative all'**accesso non autorizzato di tirocinanti alle cartelle cliniche dei pazienti**, rilevando carenze strutturali circa l'accessibilità alle cartelle cliniche da parte del personale ospedaliero.

In particolare, pur essendo previsto un sistema di rilevazione automatico degli accessi alle cartelle cliniche, non venivano svolti sufficienti controlli sulla legittimità di tali accessi e non era neppure previsto un sistema di autenticazione a due fattori (es. codice o password in combinazione con un badge personale).

Belgio: sanzione di 50.000 euro a società che distribuisce "scatole rosa" ai neo-genitori

Family Service è una società di marketing che distribuisce scatole rosa, tramite ginecologi e ospedali, che includono campioni, offerte speciali e fogli informativi per i futuri genitori.

L'istruttoria del Garante belga aveva appurato che **la società trasferiva i dati personali a terzi per fini commerciali senza un consenso specifico da parte degli interessati**, che non erano al corrente che l'invio delle scatole implicasse il trasferimento dei propri dati.

Inoltre, il fatto che le scatole fossero distribuite da ginecologi e ospedali avrebbe potuto portare i clienti a credere che l'iniziativa provenisse dal settore pubblico, e non da una società privata il cui core business è il trattamento di dati.

Informazione scientifica sul farmaco: profilare i medici in conformità alla privacy

L'approfondimento si pone l'obiettivo di fornire indicazioni alle Aziende farmaceutiche su come rendere l'attività di informazione scientifica sul farmaco il più efficiente possibile.

Un esempio è la profilazione dei medici sulle piattaforme, tanto utilizzate in questo periodo di emergenza sanitaria.

La **profilazione** non è cosa semplice, ma attuarla nel pieno **rispetto della normativa** di protezione dei dati personali può comportare un **aumento di produttività** ed **efficienza della "strategia di marketing"** ad essa sottesa.

Per approfondimenti si rimanda all'articolo
"Informazione scientifica sul farmaco: profilare i medici in conformità alla privacy"
a cura dell'Avv. Maria Livia Rizzo, Dott.ssa Federica Pucarelli

Le FAQ del Garante privacy sulla gestione dei vaccini dei dipendenti

Il Garante, con le FAQ "**Vaccinazioni dei dipendenti**" pubblicate il 17 febbraio 2021, ha chiarito che:

- **il datore di lavoro non può chiedere ai dipendenti di fornire informazioni o documenti sul proprio stato vaccinale**;
- il medico competente **non può comunicare al datore di lavoro i nominativi dei dipendenti vaccinati;**
- solo il medico competente può trattare i dati personali relativi alla vaccinazione dei dipendenti e fornire la propria valutazione in merito all'idoneità rispetto alla mansione specifica.

Garante Italiano - Vaccinazione dei dipendenti: le FAQ del Garante privacy. Principi generali e focus sugli operatori sanitari

Vedi il provvedimento

Il datore di lavoro può sapere se i dipendenti sono vaccinati?

In seguito alla pubblicazione delle FAQ sulle vaccinazioni dei dipendenti, l'approfondimento ha l'obiettivo di analizzare le **modalità con cui il datore di lavoro garantisce il rispetto degli obblighi in tema di sicurezza sui luoghi di lavoro** e contemporaneamente delle indicazioni in tema di vaccinazioni rilasciate dal Garante.

Per approfondimenti si rimanda all'articolo
"Il datore di lavoro può sapere se i dipendenti sono vaccinati?"
a cura dell'Avv. Maria Livia Rizzo, Dott.ssa Federica Pucarelli

Il fattore umano nei Data Breach: il comportamento dei dipendenti critico per il GDPR

Nell'articolo Fabio Marinello esamina il fattore umano come fattore di rischio nella violazione dei dati, riprendendo le considerazione dell'European Data Protection Board nel documento Guidelines 01/2021 on Examples regarding Data Breach Notification.

La parola chiave è prevenzione, la quale non può realizzarsi senza adeguati programmi di formazione e sensibilizzazione del personale sugli obblighi di privacy e sicurezza.

In questo frangente, può essere particolarmente utile ricordare ai dipendenti i più comuni errori e le strategie per evitarli, magari trasmettendo l'importanza di una banale politica di "clean-desk" per l'ordine di file e documenti.

L'ideale è che le buone pratiche configurino un insieme di vere e proprie procedure operative (che, tra l'altro, si prestano bene a regolari audit per la valutazione continua della loro efficacia).

Nonostante tutte le misure di sicurezza tecniche implementate in un sistema, il fattore umano continuerà sempre a rivestire un ruolo fondamentale per i rischi di violazione dati.

Da una parte, vi sono le violazioni accidentali: specialmente nelle routine del lavoro, lo svolgimento quotidiano di operazioni di trattamento aumenta la probabilità che si verifichino errori. E mentre, per certi versi, l'utilizzo di determinate tecnologie informatiche può ridurre l'incidenza d'errore, per altri continuerà ad avere valore l'acronimo "PEBKAC" ("Problem Exists Between Keyboard And Chair", ovvero "Il problema sta fra la tastiera e la sedia") diffuso tra gli informatici.

Vi sono poi le violazioni intenzionali, non sempre facilmente distinguibili dall'errore, elemento di ambiguità che rende particolarmente difficile per un Titolare del trattamento valutare con precisione le caratteristiche e i rischi delle violazioni di dati collegate al fattore umano.

Per approfondimenti si rimanda all'articolo
"Il fattore umano nei Data Breach: il comportamento dei dipendenti critico per il GDPR"
a cura del Dott. Fabio Marinello

Videosorveglianza a prova di GDPR: le FAQ del Garante

In data 3 dicembre il Garante ha reso disponibili sul proprio sito internet le FAQ in materia di videosorveglianza, contenenti informazioni di carattere generale e un modello semplificato di cartello.

Nell'articolo abbiamo sintetizzato gli adempimenti necessari per l'implementazione di un impianto di videosorveglianza.

In particolare nelle FAQ, il Garante riprende i contenuti delle Linee Guida dell'European Data Protection Board (EDPB) chiarendo i dubbi interpretativi che le stesse Linee Guida avevano creato rispetto alle precedenti Linee Guida sulla videosorveglianza del Garante del 2010.

Per approfondimenti si rimanda all'articolo
"Videosorveglianza a prova di GDPR: le FAQ del Garante"
a cura dell'Avv. Alessandra Delli Ponti

Garante Italiano - FAQ Videosorveglianza

Vedi le FAQ pubblicate dal Garante

E.D.P.B. European Data Protection Board - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video Versione 2.0 Adottate il 29 gennaio 2020

Vedi le Linee Guida E.D.P.B.

Reati Privacy e reati d.Lgs. 231/2001

L'articolo analizza il **rapporto tra l'articolo 24 bis del d.lgs 231/2001** - il quale annovera tra i reati presupposto per il sorgere della responsabilità amministrativa dell'ente i "Delitti informatici e trattamento illecito di dati" - e i **c.d. "reati privacy"**.

L'art. 24 bis, infatti, non richiama alcune delle fattispecie penali che sono contenute all'interno del Codice Privacy, ma ciò non toglie che vi siano numerose sovrapposizioni tra quest'ultimo, il GDPR e il sistema di responsabilità ex d.lgs. 231/2001.

Per quanto riguarda il GDPR, si pensi ad esempio agli obblighi di sicurezza previsti dall'art. 32: l'imprenditore dovrà porre in essere misure di sicurezza che garantiscano un livello di sicurezza adeguato al rischio del trattamento non solo in un'ottica di prevenzione della commissione di reati informatici, ai sensi del modello 231, ma anche in forza di questo articolo.

Dunque quanto emerge è l'importanza di un modello di compliance integrata, che abbia come obiettivi la prevenzione della verificazione di reati e di trattamenti illeciti di dati personali.

Per approfondimenti si rimanda all'articolo
""Reati privacy" e "reati 231": ci sono profili di sovrapposizione?"
a cura dell'Avv. Laura Asti, Avv. Alice Giannini

Organismo di Vigilanza ex D.lgs 231/2001 alla luce del GDPR. L'importanza di una compliance integrata

L'articolo approfondisce il tema della qualificazione, ai sensi del GDPR, del **ruolo soggettivo dell'organismo di vigilanza (Odv) ex sistema 231**.

Quest'ultimo infatti ha poteri di iniziativa e controllo sulle attività aziendali e, pertanto, ha accesso ad una serie di informazioni riservate dell'azienda.

La figura dell'OdV pare mal conciliarsi sia con una qualificazione quale Titolare autonomo del trattamento che quale Responsabile esterno.

Per questo motivo la ricostruzione ipotizzata è quella di considerare l'OdV quale componente interna dell'ente vigilato che, a sua volta, rimane l'unico Titolare del trattamento dei dati personali.

Anche qui ritroviamo l'insegnamento dell'articolo precedente: l'importanza per l'azienda di perseguire un modello di compliance integrato, che favorisca il funzionamento e la prevenzione dei rischi a 360 gradi.

Per approfondimenti si rimanda all'articolo
"L'Organismo di Vigilanza ex D.Lgs. 231/2001 alla luce del GDPR: l'importanza di una compliance integrata"
a cura dell'Avv. Laura Asti, Avv. David Vaccarella

UE: il Regolamento e-Privacy ha finalmente ottenuto parere favorevole dal Consiglio UE

Dopo un iter durato quattro anni, il Consiglio dell'Unione Europea ha raggiunto un accordo sulla versione finale del testo del Regolamento e-Privacy sulla tutela della vita privata e della riservatezza nell'uso di servizi di comunicazione elettronica.

La norma aggiornata sostituirà la vigente Direttiva e-Privacy del 2002 introducendo cambiamenti fondamentali per tutte le aziende operanti nell'economia digitale.

Nell'ambito di tali poteri, pertanto, l'ente decide come l'Organismo di Vigilanza deve trattare i dati personali.

Guidelines 02/2021 on Virtual Voice Assistants

L'assistente vocale virtuale (VVA) è un servizio che capisce ed esegue comandi vocali; sono presenti su una moltitudine di dispositivi utilizzati quotidianamente e fungono da interfaccia tra gli utenti e molti servizi on line.

A causa dei compiti svolti raccolgono e trattano un numero elevato di dati personali.

L'EDPB ha elaborato le Linee guida 2/2021, pubblicate il 9/3/2021 e in fase di consultazione per 6 settimane, identificando le sfide di conformità in tema di trattamento dei dati personali e fornendo raccomandazioni ai soggetti interessati su come affrontarle.

Le Linee guida raccomandano ai progettisti di VVA di assolvere l'**obbligo di informativa di cui all'art. 13 GDPR impostando l'informativa tramite voce e di prevedere la registrazione degli utenti per ogni funzione messa a disposizione dalle VVA**.

Sul consenso al trattamento dei dati l'EDPB chiarisce che nella misura in cui i dati sono trattati **per eseguire le richieste degli utenti, NON è necessario per i Titolari del trattamento acquisire il consenso**; al contrario **è obbligatorio il consenso per qualsiasi trattamento non strettamente connesso alle finalità richieste dall'utente**.

Sui tempi di conservazione le VVA non dovrebbero conservare i dati per un periodo superiore a quello necessario per conseguire le finalità per cui i dati sono trattati, indipendentemente dalle istanze di cancellazione promosse dagli utenti.

Alcuni dati possono essere raccolti dalle VVA accidentalmente, in tal caso i progettisti devono prevedere meccanismi di cancellazione automatica.

Le VVA possono trattare dati di più interessati; i progettisti devono pertanto implementare meccanismi di controllo degli accessi idonei a garantire la riservatezza, l'integrità e la disponibilità. Le Linee guida sottolineano che ad esempio le password non sono ritenute un meccanismo idoneo nel caso delle VVA, fornendo invece indicazioni specifiche in un'apposita sezione sul trattamento di categorie particolari di dati per l'identificazione biometrica.

L'esercizio dei diritti degli interessati dovrebbe essere garantito tramite semplici comandi vocali facili da utilizzare da parte degli utenti.

L'EDPB sottolinea infine che le VVA rientrano tra quei servizi per cui è necessario eseguire una

DPIA.

In attesa dell'emanazione della versione definitiva delle Linee guida, il Garante italiano ha aggiornato la propria scheda informativa sul tema.

Garante Italiano - Assistenti digitali (smart assistant): i consigli del Garante per un uso a prova di privacy

Vedi la scheda informativa del Garante

E.D.P.B. European Data Protection Board - Guidelines 02/2021 on Virtual Voice Assistants - Status: OPEN FOR FEEDBACK

Vedi le Linee Guida E.D.P.B.

Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications

L'EDPB ha pubblicato la versione definitiva delle Linee guida 1/2020, sottoposte a consultazione lo scorso anno, concernenti il trattamento dei dati personali effettuato dai veicoli connessi.

Poiché i veicoli connessi generano dati la maggior parte dei quali possono essere considerati dati personali in quanto riferibili a conducenti o passeggeri, non ci sono dubbi circa l'applicabilità al trattamento di specie delle prescrizioni di cui al GDPR ma anche della Direttiva ePrivacy; sul punto, l'EDPB espressamente chiarisce che l'"apparecchio terminale" di cui all'art. 5, par. 3, della Direttiva ePrivacy ricomprenda anche i veicoli connessi ed ogni strumento digitale connesso ai medesimi.

Le Linee Guida, in particolare, si concentrano sull'analisi:

- dei dati personali raccolti e trattati all'interno del veicolo;
- dei dati personali oggetto di interazione tra il veicolo e i dispositivi ad esso collegati;
- dei dati personali raccolti all'interno del veicolo ed esportati verso soggetti terzi per essere sottoposti a trattamenti ulteriori.

Prima di fornire una serie di raccomandazioni volte a garantire la compliance dei trattamenti dati in esame, il Comitato mette in luce i rischi che tali trattamenti potrebbero comportare per i diritti e le libertà degli interessati, rilevando innanzitutto potenziali criticità dovute ad un difetto di adeguata informazione degli interessati in virtù del fatto che, spesso, il proprietario del veicolo non coincide con l'utilizzatore dello stesso, con la conseguenza che quest'ultimo potrebbe avere delle difficoltà a ricavare informazioni sul trattamento dei propri dati ed eventualmente opporsi allo stesso.

Tale ipotesi risulterebbe ovviamente maggiormente impattante negli ambiti del noleggio veicoli e del car sharing.

Un ulteriore rischio per gli interessati potrebbe derivare dal numero sempre crescente di sensori impiegati nei veicoli connessi, comportando una raccolta di dati potenzialmente eccessiva rispetto a quanto necessario per raggiungere le finalità alla base del trattamento.

Le Linee Guida dettano una serie di raccomandazioni per i titolari e i responsabili coinvolti nei trattamenti, volte a mitigare i già indicati rischi per gli interessati.

Anzitutto, l'EDPB invita gli operatori a volgere particolare attenzione a tre categorie di dati, ovvero

- i dati di geolocalizzazione;
- i dati biometrici
- i dati suscettibili di rivelare infrazioni o violazioni del codice della strada.

Sulla prima categoria di dati, le Line Guida chiariscono che titolari e responsabili devono muovere dal presupposto che i dati di geolocalizzazione siano potenzialmente rivelatori delle abitudini di vita dei soggetti interessati; constatazione da cui discende la necessità, nell'ottica di garantire quanto più possibile il principio di minimizzazione, che tali dati non vengano sottoposti a trattamento, salvo che ciò sia assolutamente necessario per il perseguimento di specifiche finalità e comunque sempre mettendo in atto specifiche accortezze.

Suscettibili di tutela rafforzata risulteranno anche i dati biometrici dell'interessato, utilizzati ad esempio per consentire l'apertura/chiusura del veicolo, per autenticare il conducente/proprietario e/o per consentire l'accesso alle preferenze del profilo del conducente; in tali ipotesi l'EDPB suggerisce di prevedere l'esistenza di un'alternativa "non biometrica" oppure di adottare soluzioni di criptazione di tali dati, la cui conservazione deve limitarsi al dispositivo locale, evitando quindi qualunque forma di trasmissione verso un terminale esterno.

Tra le best practices applicabili, il Comitato suggerisce di dare spazio a tecniche di anonimizzazione per l'eventuale trasferimento di dati.

Altrettanto consigliato è lo svolgimento di una valutazione d'impatto.

Relativamente alle garanzie connesse all'esercizio dei diritti da parte degli interessati, l'EDPB suggerisce la predisposizione di tool specifici che agevolino tale esercizio e, in particolare, l'implementazione di un "profile management system" all'interno del veicolo che, centralizzando tutte le impostazioni connesse al trattamento dati, permetta, con facilità, l'accesso, la cancellazione e la rimozione dei dati personali dai sistemi del veicolo su richiesta dell'interessato e, in più, abiliti quest'ultimo ad interrompere la raccolta di alcuni tipi di dati, temporaneamente o permanentemente, in qualsiasi momento, a meno che una specifica legislazione non preveda diversamente o i dati

risultino essenziali per il funzionamento del veicolo.

Infine rileviamo che l'EDPB ha espressamente invitato gli operatori del settore automobilistico (in particolare le aziende costruttrici) a munirsi di un codice di condotta che, recependo le indicazioni riportate all'interno delle Linee Guida, possa migliorare l'applicazione in ogni processo dei principi di privacy by design e by default, in conformità ai quali sarebbe opportuno prevedere che le tecnologie alle base dei veicoli connessi risultino sin dalla fase di progettazione concepite in modo da ridurre al minimo la raccolta di dati personali, fornire impostazioni predefinite di protezione dei dati personali e garantire che gli interessati, oltre ad essere adeguatamente informati, siano muniti della possibilità di modificare facilmente ogni impostazione associata ai propri dati personali assicurando un'adeguata protezione per i diritti e le libertà degli interessati sin dalla fase di progettazione del veicolo e quindi del trattamento dei dati.

E.D.P.B. European Data Protection Board - Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications

Vedi le Linee Guida E.D.P.B.

STEFANELLI & STEFANELLI STUDIO LEGALE

il valore del network

la forza dell'esperienza

LO STUDIO

AVV. ANDREA STEFANELLI
AVV. SILVIA STEFANELLI

AVV. FABIO CARUSO
AVV. GASPARE CASTELLI
AVV. ADRIANO COLOMBAN
AVV. MADDALENA COLLINI
AVV. ALESSIA DIOLI
AVV. ALESSANDRA DI NUNZIO
AVV. ALICE GIANNINI
AVV. ELEONORA LENZI
AVV. SILVIA PARI
AVV. ELEONORA PETTAZZONI
AVV. MARIA LIVIA RIZZO
AVV. GIORGIA VERLATO

DOTT. SSA CAMILLA ANDERLINI
DOTT.SSA NOEMI CONDITI
DOTT. SSA ILARIA NANNI
DOTT.SSA FEDERICA PUCARELLI

AVV. LAURA ASTI of counsel
AVV. FEDERICO BRESCHI of counsel
AVV. ALESSANDRA DELLI PONTI of counsel
AVV. ANDREA MARINELLI of counsel
PROF. AVV. ALESSANDRA MAGLIARO of counsel

LE AREE DI SPECIALIZZAZIONE

APPALTI
SANITÀ
IMPRESE
DISPOSITIVI MEDICI
PRIVACY
NUOVE TECNOLOGIE
LAVORO
COMPLIANCE D.LGS. 231/2001
PENALE COMMERCIALE
TRIBUTARIO
COMMERCIALE INTERNAZIONALE
DISTRIBUZIONE E RETAIL