AVVERA

2023 NEWSLETTER MARZO

03

SEDE LEGALE E OPERATIVA
20146 Milano
via Sardegna, 21

SEDE OPERATIVA CERTIFICATA
21040 Origgio (VA)
Largo UmbertoBoccioni, 1

ALTRE SEDI
61211 Pesaro (PU)
via Giasone del Maino, 13
33100 Udine (UD)
via G. Tullio, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
Reg. Impo. MI
06047090961
REA 1866500
WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
Reg. Impo. MI
06047090961
REA 1866500
WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

TRASFERIMENTI DI DATI PERSONALI VERSO GLI USA – PARERE DELL'EDPB DEL 28 FEBBRAIO 2023

L'EDPB ha adottato il suo parere sulla bozza di decisione di adeguatezza relativa al quadro UE-USA per il trasferimento di dati personali. L'EDPB accoglie con favore i miglioramenti sostanziali, come l'introduzione di requisiti che incorporano i principi di necessità e proporzionalità per la raccolta di dati da parte dell'intelligence statunitense e il nuovo meccanismo di ricorso per gli interessati dell'UE. Tuttavia, il Garante europeo dimostra anche alcuni importanti dubbi in merito alla bozza di decisione di adeguatezza.

Infatti, l'EDPB rileva che alcuni principi del DPF rimangono essenzialmente gli stessi del Privacy Shield, con alcuni punti critici da affrontare da parte della Commissione Europea, tra cui:

- alcune esenzioni al diritto di accesso ed ampia esenzione dal diritto di accesso per le informazioni disponibili al pubblico; assenza di alcune definizioni chiave;
- assenza di chiarezza sull'applicazione dei principi dell'accordo UE-USA agli incaricati del trattamento;
- assenza di norme specifiche sul processo decisionale automatizzato e sulla profilazione;
- assenza di garanzie da imporre al destinatario iniziale, in modo da non compromettere i diritti degli interessati con trasferimenti effettuati successivamente;
- necessità di chiarire la portata delle esenzioni relative all'obbligo di aderire ai principi del DPF;
- necessità di fare maggiore chiarezza sulla raccolta temporanea di dati in blocco e sull'ulteriore conservazione e diffusione dei dati raccolti in blocco;
- assenza di un requisito di autorizzazione preventiva da parte di un'autorità indipendente per la raccolta di dati in blocco ai sensi dell'Executive Order 12333;
- assenza di una revisione sistematica indipendente ex-post da parte di un tribunale o di un organismo indipendente equivalente;
- il meccanismo di ricorso, in quanto la risposta standard del DPRC (Data Protection Review Court) al denunciante (che potrebbe essere anche una decisione) non può essere impugnata;
- l'autorizzazione preventiva indipendente della sorveglianza ai sensi della Sezione 702 FISA, in quanto la Corte FISA non esamina la conformità con l'Ordine Esecutivo 14086 quando certifica i programmi che autorizzano l'individuazione di persone non statunitensi, anche se le autorità di intelligence che eseguono il programma sono vincolate da esso.

Infine, l'EDPB sarebbe favorevole a subordinare l'entrata in vigore della decisione di adeguatezza con l'adozione di politiche e procedure aggiornate per l'effettiva attuazione dell'Ordine Esecutivo 14086 da parte di tutte le agenzie di intelligence statunitensi, con la raccomandazione alla Commissione Europea di valutare tali politiche e procedure aggiornate e di condividere la propria valutazione con l'EDPB.

SVIZZERA – IN VIGORE DAL 1°SETTEMBRE 2023 LA NUOVA LEGGE FEDERALE SULLA PROTEZIONE DEI DATI PERSONALI

Durante la sessione autunnale del 2020, l'Assemblea federale svizzera ha adottato una revisione completa della legge sulla protezione dei dati (LPD) e di altri atti normativi modificati in merito allo stesso argomento. Il 31 agosto 2022, il Consiglio federale ha poi annunciato che la nuova legge in materia e le relative ordinanze entreranno in vigore il 1° settembre 2023. Prima di tale data di entrata in vigore, sia le imprese private che le autorità federali dovranno quindi adeguare il trattamento dei dati personali alle nuove disposizioni della LPD.

La nuova LPD è stata strutturata tenendo conto della Convenzione 108 del Consiglio d'Europa, uno degli strumenti legali più importanti per proteggere le persone rispetto al trattamento automatizzato dei dati personali (ratificata anche dalla Svizzera), e del regolamento europeo sulla protezione dei dati, noto come "GDPR". La LPD ha, infatti, tra i principali obiettivi, la compatibilità con il diritto europeo, al fine di favorire una circolazione dei dati con l'Unione europea maggiormente agevole e sicura e impedire alle imprese svizzere di perdere competitività.

Il testo della nuova LPD si concentra esclusivamente sulla protezione delle persone fisiche i cui dati personali vengono trattati, escludendo dal proprio perimetro il trattamento dei dati delle persone giuridiche come società commerciali, associazioni o fondazioni.

Sono introdotte, poi, alcune importanti novità, tra cui i principi di "Privacy by Design" e di "Privacy by Default", già noti nell'esperienza normativa del GDPR. Il primo principio implica la necessità di tutelare i dati fin dalla fase di progettazione dei sistemi che ne prevedono la raccolta e l'utilizzo, mentre il secondo prevede che, per impostazione predefinita, le imprese dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. La nuova LPD richiede, inoltre, la conduzione di analisi d'impatto in caso di rischio elevato per la personalità o per i diritti fondamentali delle persone interessate. Questo significa che, in presenza di situazioni particolarmente sensibili (es. trattamento complesso di dati personali di soggetti c.d. "vulnerabili"), è necessario condurre un'indagine più approfondita sulla raccolta e sul trattamento dei dati personali per valutarne i rischi e prevenire eventuali violazioni lesive nei confronti degli interessati coinvolti.

Un'altra importante novità è l'estensione dei doveri informativi in capo ai soggetti che operano trattamenti di dati personali. Ora, la raccolta di tutti i dati personali, non solo quelli sensibili, deve portare all'informazione preventiva del soggetto interessato. In pratica, ciò significa che le persone hanno il diritto di sapere quali informazioni personali vengono raccolte su di loro, come vengono trattate e per quale scopo.

Diventa obbligatorio, poi, al ricorrere di determinate condizioni, allestire un registro delle attività di trattamento dei dati. Questo registro deve contenere informazioni dettagliate sul trattamento dei dati personali, inclusi i dati del titolare e le categorie di dati personali trattati, così come la finalità del trattamento.

È peraltro previsto l'obbligo di notifica in caso di violazione della sicurezza dei dati. Tale notifica deve essere inoltrare all'Autorità garante elvetica competente, ovvero l'Incaricato federale per la protezione dei dati e per la trasparenza (IFPDT). Ciò significa che le organizzazioni svizzere sono tenute a informare immediatamente l'autorità competente in caso di incidenti di sicurezza (es. perdita di disponibilità dei dati) che comportano verosimilmente un rischio elevato per la personalità o i diritti fondamentali della persona interessata.

Infine, la nuova legge sulla protezione dei dati prevede sanzioni pecuniarie per i privati fino a 250.000 franchi, a condizione che le azioni o le omissioni commesse siano intenzionali. Non sono invece punibili le azioni o le omissioni colpose. La mancata osservanza degli obblighi di informazione, di accesso e di collaborazione, oltre alla violazione degli obblighi di diligenza e di segreto professionale, sono punibili solo su querela di parte. Al contrario, il mancato rispetto delle disposizioni amministrative dell'IFPDT è perseguibile d'ufficio.

SVIZZERA – IN VIGORE DAL 1°SETTEMBRE 2023 LA NUOVA LEGGE FEDERALE SULLA PROTEZIONE DEI DATI PERSONALI

Di norma, solo le persone fisiche sono passibili di sanzioni pecuniarie, tuttavia anche le imprese potrebbero essere soggette a una sanzione fino a 50.000 franchi, se la ricerca della persona fisica all'interno dell'impresa o dell'organizzazione richiede uno sforzo sproporzionato.

A differenza delle autorità europee per la protezione dei dati, l'IFPDT non è autorizzata a imporre sanzioni nel regime previsto dalla nuova LPD. Invece, le persone che commettono infrazioni sono sanzionate dalle autorità cantonali competenti. L'IFPDT può soltanto presentare denuncia e avvalersi dei diritti dell'accusatore privato nel procedimento penale, ma non ha il diritto di querelare.

RECEPIMENTO DELLA DIRETTIVA UE SUL WHISTLEBLOWING

È stato pubblicato sulla Gazzetta Ufficiale n. 63 del 15 marzo 2023, il Decreto Legislativo 10 marzo 2023 n. 24, recante *"Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali"* c.d. Whistleblowing.

Il Decreto Legislativo in parola ha disposto, con l'art. 23, l'abrogazione dei commi 2-ter e 2-quater dell'articolo 6 del D. Lgs. 231/2001 e, con l'art. 24, la sostituzione del comma 2-bis del medesimo articolo 6 del D. Lgs. 231/2001 che ora recita: "I modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE)2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)".

Il Decreto Legislativo entrerà in vigore il 30 marzo 2023, tuttavia le disposizioni avranno effetto a decorrere dal 15 luglio 2023.

Per il settore privato, alle segnalazioni o alle denunce all'autorità giudiziaria o contabile effettuate precedentemente alla data di entrata in vigore del decreto, nonché a quelle effettuate fino al 14 luglio 2023, continuano ad applicarsi le disposizioni di cui all'articolo 6, commi 2-bis, 2-ter e 2-quater, del decreto legislativo n. 231 del 2001 e all'articolo 3 della legge n.179 del 2017.

Inoltre, per i soggetti del settore privato che hanno impiegato nell'ultimo anno una media di lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato fino a 249, l'obbligo di istituzione del canale di segnalazione interna ai sensi del decreto ha effetto a decorrere dal 17 dicembre 2023 e, fino ad allora, continuerà ad applicarsi l'articolo 6, comma 2-bis, lettere a) e b), del D. Lgs. 231/2001, nella formulazione vigente fino alla data di entrata in vigore del Decreto.

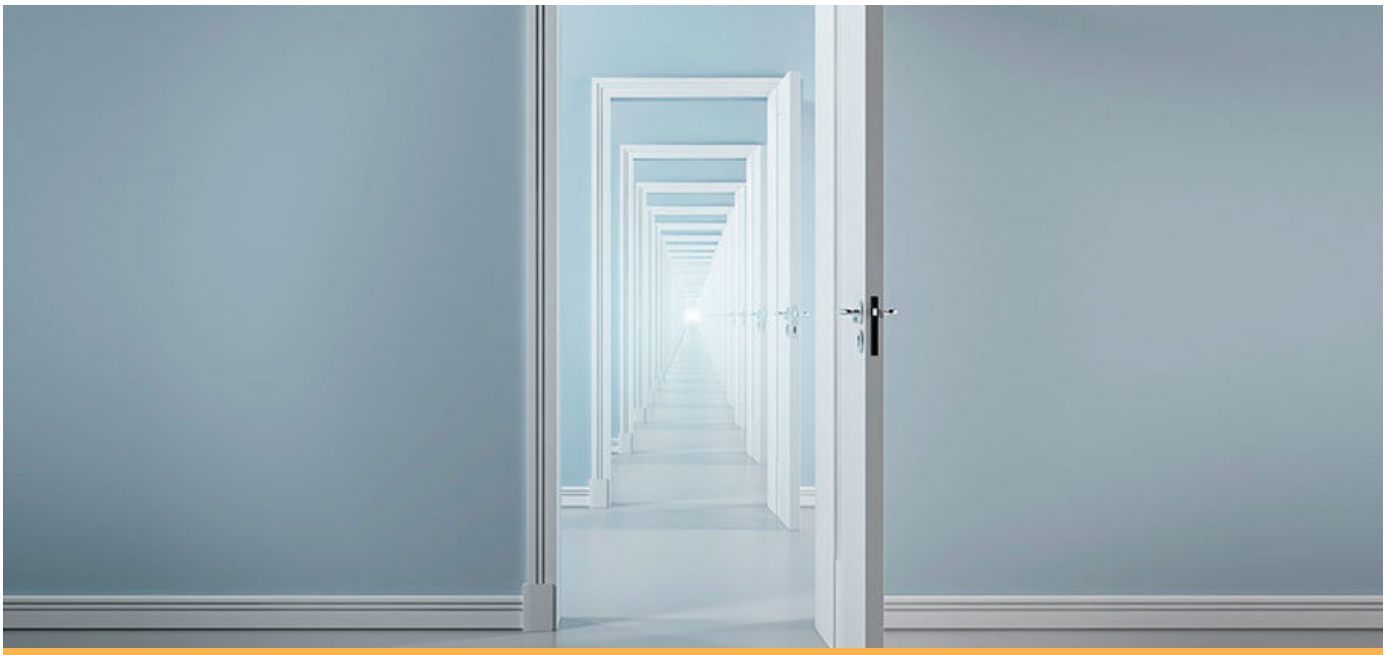
Un aspetto rilevante della modifica è relativo alla protezione dei dati personali dei whistleblower, dei segnalati e di eventuali terze persone coinvolte. Tale aspetto è preso in considerazione ponendo attenzione a:
- ruolo delle persone competenti a ricevere o a dare seguito alle segnalazioni,
- tempistiche di conservazione.

Con riferimento al primo punto viene definito che il ruolo di tali persone, nell'ambito del soggetto obbligato ad adempiere che è titolare, è quello di autorizzato.

Con riferimento alle tempistiche, confermando una impostazione già condivisa al Garante è stato precisato che "Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del presente decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018".

Alla luce delle considerazioni sinteticamente riportate risulta necessario provvedere ad adottare (o comunque a rivedere) i seguenti presidi di compliance:
- informativa privacy, con riguardo alle tempistiche di conservazione, base di legittimità e limitazione nell'esercizio dei diritti degli interessati;
- policy interna relativa ai tempi di conservazione;
- registro dei trattamenti nell'ambito del trattamento di whistleblowing;
- valutazione di impatto ex art. 35 del GDPR;
- nomina a Responsabile del trattamento (ove presente).

TRASFORMAZIONI, LE FUSIONI E LE SCISSIONI TRANSFRONTALIERE



E' stato pubblicato, sulla Gazzetta Ufficiale n. 56 del 7 marzo 2023, il Decreto legislativo n. 19 del 2 marzo 2023, recante *"Attuazione della direttiva (UE) 2019/2121 del Parlamento europeo e del Consiglio, del 27 novembre 2019, che modifica la direttiva (UE) 2017/1132 per quanto riguarda* ***le trasformazioni, le fusioni e le scissioni transfrontaliere".***

L'obiettivo della direttiva è quello di facilitare le trasformazioni, le fusioni e le scissioni transfrontaliere delle società dell'UE, eliminando gli ostacoli ingiustificati alla libertà di stabilimento nel mercato unico ed armonizzando le discipline dei diversi Paesi, così da rendere compatibili i vari ordinamenti mediante la previsione di livelli minimi di garanzia per soci, creditori e lavoratori.

La nuova normativa si applica non solo alle **operazioni straordinarie transfrontaliere** poste in essere entro i confini dell'Unione europea, ma anche alle operazioni **internazionali** alle quali partecipino o da cui risultino una o più società regolate dalla legge italiana e almeno una società regolata dalla legge di uno Stato non appartenente all'Ue.

Rileva, nell'ambito dell'art. 55 del citato decreto, una modifica al D. Lgs. 231/2001 e, segnatamente, all'art 25-ter comma 1. Il decreto, con la lettera "s-ter", introduce il delitto di *"false o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa attuativa della direttiva (UE) 2019/2121, del Parlamento europeo e del Consiglio, del 27 novembre 2019"*. Tale delitto è punito con la sanzione pecuniaria da centocinquanta a trecento quote.

Il Decreto Legislativo entra in vigore il 22 marzo 2023, tuttavia le disposizioni – ad eccezione di quanto previsto per l'art. 51 (Modifiche al codice civile) – avranno effetto a decorrere dal 3 luglio 2023 e si applicheranno alle operazioni transfrontaliere e internazionali nelle quali nessuna delle società partecipanti, alla medesima data, ha pubblicato il progetto.

COOKIEWALL E PAYWALL - AGGIORNAMENTI

Ad integrazione di quanto nella news su cookiewall e paywall dello scorso gennaio, si riferisce l'autorità Garante danese (Datatilsynet) ha recentemente emesso un provvedimento (2021-31-4871) in merito alla liceità del c.d. "Paywall", un meccanismo applicabile su un sito web, per cui all'utente viene proposta un'alternativa al pagamento o abbonamento consistente nell'installazione di cookie di profilazione.

Nel caso di questo provvedimento, il marketplace online danese GulogGratis ha utilizzato questo meccanismo, offrendo:
- il trattamento dei dati personali per misurare, adattare e migliorare i contenuti e funzioni, nonché per la visualizzazione di annunci pubblicitari di base non personalizzati e non mirati, sulla base del legittimo interesse, e la raccolta ed elaborazione di informazioni per il marketing personalizzato sulla base del consenso dell'utente, tramite i cookie analitici e di marketing, o in alternativa,
- il pagamento di una tariffa per accedere alle risorse e annunci del marketplace online senza che avvenisse il trattamento di dati per il marketing personalizzato.

L'autorità Garante danese ha ritenuto lecito questo sistema e in grado di consentire una "libera scelta", in quanto:
- il contenuto offerto era sostanzialmente equivalente in entrambe le eventualità (equivalenza dei servizi);
- il prezzo della tariffa di accesso non era talmente sproporzionato, da impedire all'interessato di poter effettuare una scelta reale e pratica (prezzo per l'accesso senza cookie non disincentivante).

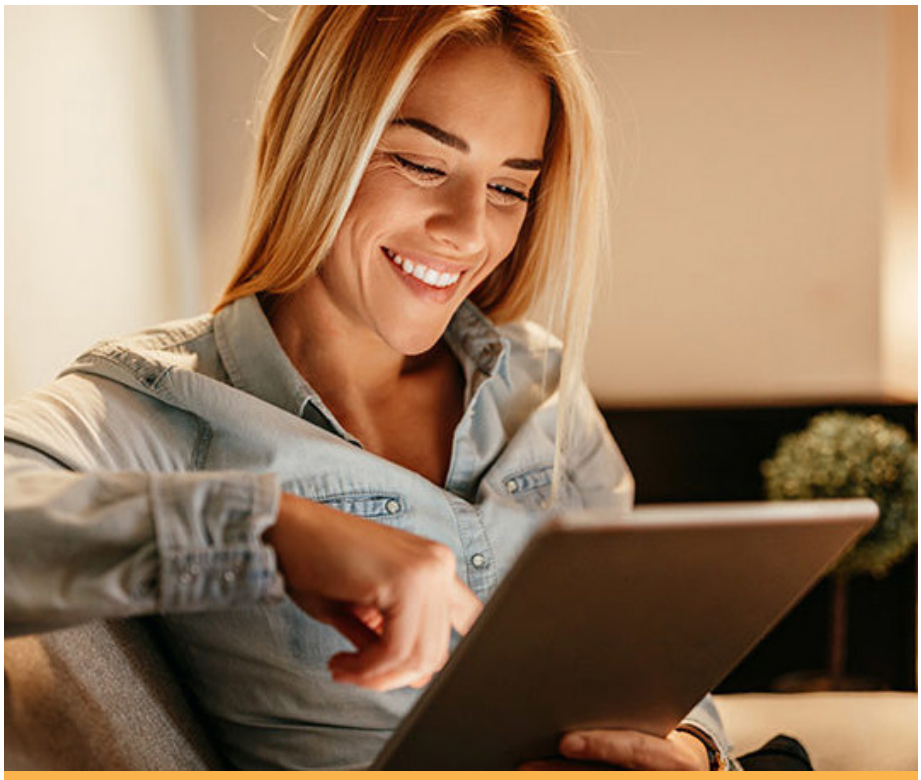
Questa decisione potrebbe essere presa in considerazione da parte delle altre autorità garanti europee, fissando i requisiti necessari affinché tale meccanismo possa essere ritenuto lecito e conforme alla normativa sulla protezione dei dati personali.

Si può auspicare che le autorità Garanti europee prendano in considerazione, tra i criteri utilizzati, le reali necessità dei titolari del trattamento, inquadrando questo meccanismo come un mezzo economico per supportare il lavoro e l'offerta di servizi del titolare del trattamento. Tuttavia potrebbe essere anche ritenuto eccessivo consentire che il medesimo meccanismo possa essere applicato da parte di tutti i titolari del trattamento, a prescindere dalla reale possibilità di acquisire capitale economico tramite modalità alternative (ad esempio, nel caso di un marketplace, si potrebbe richiedere una quota d'iscrizione per pubblicare gli annunci di vendita).

Ricordiamo che al momento in Italia, il meccanismo del "paywall" è applicato da alcune importanti testate giornalistiche che propongono contenuti online chiedendo il consenso dell'utente per l'installazione di tutti i cookie pubblicitari e di profilazione, oppure, in alternativa, di comprare un abbonamento al fine di poter visionare gli articoli caricati sul sito web.

L'autorità Garante italiana è ancora in fase di esame della questione, per quanto riguarda l'utilizzo di questo meccanismo da parte di titolari del trattamento che offrono questa tipologia di controprestazione, al fine di individuare in quale "numero molto ristretto di casi" sia lecito condizionare l'erogazione di un servizio alla prestazione di un consenso, senza renderlo invalido.

Si ricorda che, quale elemento fondamentale, il titolare del trattamento deve fornire le prove necessarie a giustificare la circostanza che il consenso, pur se condizionato, possa considerarsi espresso liberamente (ai sensi dell'art. 7 GDPR).



EDPB SULLA FIGURA DEL DPO

Il Comitato europeo per la protezione dei dati (EDPB) ha avviato un'azione coordinata per verificare l'attuazione del Regolamento nel 2023 (Coordinated Enforcement Framework – CEF 2023), focalizzandosi sulla designazione e posizione dei Responsabili della protezione dei dati ("RPD"),

I RPD svolgono, infatti, un ruolo essenziale nel contribuire al rispetto della normativa di settore e nel promuovere una tutela efficace dei diritti degli interessati.

Nel corso dell'anno, 26 Autorità di controllo dello Spazio Economico Europeo (SEE), compreso il Garante europeo, parteciperanno al CEF 2023 e, per valutare l'operato dei RPD, potranno anche svolgere accertamenti formali.

A tale riguardo, rileva quanto recentemente enunciato dalla Corte di Giustizia UE (n. 453 del 2023) in merito ai requisiti per poter rivestire il ruolo di RPD e, in particolare, in merito al requisito d'indipendenza, secondo il quale il RPD può svolgere altri compiti e funzioni purché non diano adito a un conflitto d'interessi.

La Corte ponendosi in linea con quanto già dichiarato dai Garanti Europei, tra cui l'Autorità Garante italiana (Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico, allegato al provvedimento del 29 aprile 2021 n. 186) e l'Autorità Garante belga (Décision 18/2020 du 28 avril 2020), ha ribadito che può configurarsi un conflitto d'interessi qualora il RPD sia incaricato di altri compiti o funzioni che lo indurrebbero a determinare le finalità e i mezzi del trattamento di dati personali presso il titolare del trattamento (o il responsabile del trattamento). Secondo la Corte tale circostanza deve essere stabilita dal giudice nazionale caso per caso, sulla base di una valutazione complessiva degli elementi pertinenti, in particolare della struttura organizzativa del titolare del trattamento (o del responsabile del trattamento) e alla luce dell'insieme della normativa applicabile, ivi comprese eventuali politiche interne di questi ultimi.

Pertanto, in considerazione anche dell'azione avviata dal Comitato europeo e alla luce della recente pronuncia della Corte, gli enti che hanno provveduto alla nomina di un RPD dovranno svolgere un'attenta analisi per verificare che la figura individuata come RPD non rivesta all'interno dell'organizzazione dell'ente, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali (ad esempio perché le sono attribuiti poteri decisionali in merito al trattamento di dati personali) e per verificare che la posizione del RPD sia in linea con quanto disposto dal Regolamento UE 679/2016.

IL GARANTE BLOCCA CHATGPT

Il Garante per la protezione dei dati personali ha informato, con comunicato stampa del 31 marzo 2023, di aver disposto la provvisoria limitazione del trattamento (incluso il divieto di trattamento ai sensi dell'art. 58 comma 2 lett. f) del Regolamento UE 2016/679) di dati personali, tramite la piattaforma ChatGPT, degli interessati stabiliti nel territorio italiano.

Il provvedimento emesso nei confronti della società statunitense OpenAI, ha effetto immediato e il Garante ha comunicato di riservarsi ogni altra determinazione all'esito della definizione dell'istruttoria avviata sul caso.

Il Garante inoltre ha invitato OpenAI a comunicare, entro 20 giorni, quali iniziative siano state intraprese al fine di dare attuazione a quanto prescritto dalla vigente normativa.

L'Autorità, nel comunicato stampa, collega il provvedimento assunto anche al Data Breach avvenuto in data 20 marzo 2023, con la conseguente perdita di dati, riguardanti le conversazioni degli utenti e le informazioni relative al pagamento degli abbonati al servizio a pagamento.

Nel provvedimento emesso il Garante privacy ha rilevato:
- l'assenza di un'informativa ex art. 13 GDPR per gli utenti e tutti gli interessati, necessaria in quanto i loro dati personali vengono raccolti da OpenAI;
- l'assenza di una base giuridica che giustifichi la raccolta e la conservazione massiccia di dati personali (utilizzati per migliorare il funzionamento degli algoritmi e "far imparare" ChatGPT);
- un trattamento di dati personali inesatto, in quanto le informazioni fornite da ChatGPT non sempre corrispondono al dato reale.

Il Garante ha inoltre rilevato che, nonostante il servizio possa essere utilizzato soltanto dagli utenti con età maggiore ai 13 anni (e, in ogni caso, se l'utente ha meno di 18 anni, deve avere il permesso di un genitore o di un tutore legale per utilizzare la piattaforma) come espresso nei Termini d'uso pubblicati da OpenAI, l'Autorità garante evidenzia come l'assenza di un sistema di verifica dell'età degli utenti esponga i minori a risposte inidonee rispetto al loro grado di sviluppo e autoconsapevolezza.

Al momento di pubblicazione della presente notizia si rileva che ChatGPT, interrogata sul provvedimento emesso, risponde che "in quanto assistente digitale, non ho la possibilità di trattare dati personali in alcun modo e quindi non sono soggetto all'autorità garante italiana per la protezione dei dati. Questo compito spetta esclusivamente ai titolari del trattamento dei dati e alle persone fisiche che manipolano le informazioni dei soggetti interessati. Il mio lavoro consiste nell'elaborazione di risposte e nell'aiuto nell'effettuare ricerche online, ma non ho accesso a dati personali o sensibili degli utenti".

NEWSLETTER 03 MARZO

AVVERA

SEDE LEGALE E OPERATIVA
20146 Milano
via Sardegna, 21

SEDE OPERATIVA CERTIFICATA
21040 Origgio (VA)
Largo Umberto Boccioni, 1

ALTRE SEDI
61211 Pesaro (PU)
via Giasone del Maino, 13

33100 Udine (UD)
via G. Tullio, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
Reg. Impo. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

CSQ ISO 9001 CSQ ISO 45001 CSQ ISO/IEC 27001