Ordinanza ingiunzione nei confronti di Senseonics Inc. - 7 luglio 2022 [9809998]

VEDI ANCHE NEWSLETTER DEL 3 OTTOBRE 2022

[doc. web n. 9809998]

Ordinanza ingiunzione nei confronti di Senseonics Inc. - 7 luglio 2022

Registro dei provvedimenti
n. 242 del 7 luglio 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stazione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito "Regolamento");

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), come modificato dal d.lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al citato Regolamento (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, in www.gpdp.it, doc. web n. 1098801;

Relatore il dott. Agostino Ghiglia;

PREMESSO

1. La violazione dei dati personali

In data XX, la società statunitense Senseonics Inc (di seguito "Senseonics" o la "Società) ha notificato una violazione di dati personali, ai sensi dell'art. 33 del Regolamento.

La violazione, è consistita nell'invio "Nel contesto di una campagna informativa in merito alla distribuzione in Italia di Eversense XL - un sistema di monitoraggio continuo del glucosio per persone affette da diabete –di una email istituzionale "a delimitati gruppi di clienti Eversense XL inserendo gli indirizzi email dei destinatari nel campo "cc" invece che nel campo "bcc". Conseguentemente, ciascun destinatario ha avuto la possibilità di prendere visione degli indirizzi di posta elettronica degli altri destinatari della email istituzionale". La violazione ha riguardato circa 2000 interessati italiani ed è stata causata da un errore involontario da parte di un dipendente della Società.

Più nello specifico, è stato rappresentato che "L'incidente notificato comporta la possibilità per terzi non autorizzati di accedere a indirizzi email di persone potenzialmente interessate a prodotti per il diabete, ovvero agli indirizzi email dei loro caretaker. Tali indirizzi email sono in alcuni casi costituiti da una combinazione di nome e cognome che rende così possibile l'identificazione del soggetto in questione, divulgando indirettamente dati relativi alla sua salute, ovverosia una categoria particolare di dati personali ai sensi dell'Art. 9 del RGPD".

È stato inoltre rappresentato che la Società "adotta misure tecniche e organizzative standard di settore per garantire la sicurezza e protezione dei dati. In particolare, sono adottate le seguenti misure: sensibilizzazione e formazione, firewall, crittografia, policy in tema di privacy, controllo logico degli accessi, autenticazione di rete, regolari aggiornamenti software, log degli accessi e sistemi di anti-malware".

La violazione è stata comunicata agli interessati coinvolti attraverso l'invio di una mail di scuse che conteneva: "[la] descrizione della violazione; [i] recapiti in caso di domande o problemi; [la] descrizione delle possibili conseguenze della violazione e delle misure per porre rimedio alla violazione [e] (…) per mitigare possibili effetti negativi per gli interessati". Tramite tale comunicazione ai destinatari è stato altresì chiesto di cancellare l'email ricevuta con indirizzi "in chiaro".

Inoltre, per prevenire simili violazioni future, la Società ha rappresentato che "sta attualmente valutando una completa revisione dei processi di comunicazione con gli utenti e provvederà, ove lo ritenga necessario, a rafforzare le misure di sicurezza tecniche e organizzative utili ad assicurare che tali violazioni non avvengano in futuro. Senseonics sta inoltre valutando la possibilità di implementare ulteriori processi di controllo e monitoraggio delle comunicazioni con gli utenti, nonché di predisporre sistemi e/o servizi specializzati in grado di automatizzare i processi di comunicazione con gli utenti, previo settaggio di parametri adeguati, al fine di prevenire quanto più possibile l'errore umano".

2. L'attività istruttoria

Con specifico riferimento ai fatti oggetto della suddetta violazione, la Società con nota del XX, ha fornito riscontro alla richiesta di informazioni dell'Ufficio, del XX (prot. n. XX) e, ad integrazione di quanto già comunicato, ha rappresentato in atti che:

- "Abbiamo ritenuto importante che i pazienti che stavano in quel momento utilizzando Eversense (…) fossero informati del ruolo di supporto di Ascenia in modo da (…) ricevere supporto tecnico e sapere chi contattare per continuare la loro terapia Eversense. (…) l'email è stata redatta chiaramente senza finalità promozionali, ma per indicare come soddisfare le esigenze di assistenza dei clienti";

- "di aver recentemente nominato il rappresentante ai sensi dell'art. 26 del Regolamento: EDPO con sede in Avenue Huart Hamoir, 71, 1030 Bruxelles, Belgio e che sono in corso gli aggiornamento dell'Informativa privacy";

- di aver fornito con regolarità ai propri dipendenti, linee guida e istruzioni sulla protezione dei dati personali, in particolare a quelli che “gestiscono ed elaborano i dati dei pazienti e che comunicano direttamente con i pazienti” (…). La formazione e le linee guida sono state effettivamente seguite dal dipendente, ma un semplice errore umano ha causato l’incidente. Continueremo a fornire linee guida e istruzioni con regolarità e con le misure e precauzioni aggiuntive che abbiamo adottato per le comunicazioni con i pazienti, siamo fiduciosi che questo incidente sarà evitato in futuro".
Con specifico riferimento alle misure concretamente adottate al fine di evitare il ripetersi dell’evento occorso, la Società ha rappresentato che:

- “Senseonics normalmente effettua poche, se non nessuna comunicazione diretta agli utenti (…).

Per tali occasionali comunicazioni come accorgimento ulteriore richiederemo (come abbiamo fatto con l’email correttiva) una mail di conferma che la pratica di includere gli indirizzi nel campo ccn sia eseguita correttamente”.

Inoltre, la Società, in riscontro alla richiamata richiesta di informazioni, volta anche a verificare i presupposti di liceità dei trattamenti effettuati e il rispetto dei principi di correttezza e trasparenza e di integrità e riservatezza dei dati, ha fornito ulteriori elementi sul funzionamento del sistema proprietario di monitoraggio del glucosio attraverso l’applicazione mobile Eversense XL. A tale riguardo, è stato descritto il processo di download della App che viene “scaricata (su iPhone e smartphone Android), installata e utilizzata, ma solo dopo aver accettato le relative condizioni legali di Senseonics (l'Accordo di Licenza con l'Utente Finale (EULA) e l'Informativa sulla privacy e condizioni di utilizzo ("Informativa sulla privacy")”. L’installazione della App si svolge attraverso le seguenti fasi:

“Fase 1: Prima di scaricare l'App nell'app store, l'utente è in grado di rivedere l’Informativa privacy all'interno dell'app store (si veda Allegato 1). L'Informativa sulla privacy può anche essere consultata online sul nostro sito web Eversense (vedi https://global.eversensediabetes.com/privacy-policy).

Fase 2: Una volta scaricata, all'utente viene chiesto di attivare il bluetooth (per la connessione con il trasmettitore intelligente Eversense), e di accettare di ricevere gli avvisi (permettendo all'utente, ad esempio, di essere avvisato riguardo ai suoi livelli di glucosio).

Fase 3: Prima di poter creare un account ed utilizzare l'App, all'utente viene richiesto di accettare l'EULA. L'EULA fa di nuovo riferimento all'Informativa sulla privacy e riassume anche gli elementi principali dell'Informativa sulla privacy (art. 1.5 dell'EULA).

Fase 4: Una volta che l'utente clicca sul pulsante di accettazione, compare una finestra pop-a copertura dello schermo del dispositivo mobile (si veda Allegato 2), che chiede all'utente di autorizzare esplicitamente la conservazione, il trasferimento e l’utilizzo dei suoi dati personali, inclusi la conservazione dei dati nel Regno Unito e il trasferimento negli Stati Uniti per scopi limitati (come il supporto tecnico per i clienti e per soddisfare alcuni requisiti normativi), secondo quanto previsto dall’EULA e dall’Informativa sulla privacy, e, quindi, di confermare nuovamente di aver aderito all’EULA e all’Informativa sulla privacy.

Fase 5: Una volta che l'utente ha spuntato il pulsante di accettazione, viene guidato alla sezione per la creazione dell'account.

Fase 6: L'utente deve completare un modulo compilando il suo nome, cognome, indirizzo e-mail e dovrà anche creare una password. Prima di inviare, l'utente dovrà spuntare una casella per confermare che ha accettato i Termini e Condizioni e confermare, spuntando

un’apposita casella, di avere più di 18 anni (…)”.

La Società ha poi prodotto in atti una tabella nella quale sono elencate diverse finalità dei trattamenti effettuati attraverso l’utilizzo del sistema di monitoraggio del glucosio Eversense XL e la App Mobile Eversense indicando le diverse basi giuridiche di seguito riportate:

- per “la fornitura di un servizio/Assistenza clienti” le basi giuridiche del trattamento sono rinvenute nell’art. 6, par. 1, lett. b) del Regolamento e nel consenso, in caso di dati relativi alla salute (art. 9, par. 2 lett. a) del Regolamento);

- per “il miglioramento del prodotto (sviluppare e migliorare prodotti e servizi; migliorare o modificare i servizi”, le basi giuridiche sono state individuate nel legittimo interesse del titolare (art. 6, par. 1, lett. f) del Regolamento; nel consenso nel caso di dati relativi alla salute (art. 9, par. 2, lett. a) del Regolamento);

- per “marketing: analisi dei dati, invio email e avvisi ai nostri clienti riguardo ad opportunità relative ai nostri prodotti e servizi”, le basi giuridiche sono rappresentate dal “legittimo interesse al marketing diretto (art. 21.2. GDPR); opt-out delle email commerciali indirizzate a soggetti già clienti, art. 13 Direttiva E-privacy)”.

Con specifico riferimento alle informazioni fornite agli interessati, ai sensi degli artt. 13 del Regolamento, la Società ha trasmesso in atti un documento denominato “Informativa sulla privacy e condizioni di utilizzo. Data di entrata in vigore: agosto 2016. Ultima modifica: gennaio 2021”.

Sulla base degli elementi acquisiti, attraverso la comunicazione della violazione di dati personali nonché nell'ambito dell'istruttoria preliminare, l’Ufficio, con atto del XX (prot. n. XX), notificato in pari data mediante posta elettronica certificata, che qui deve intendersi integralmente riprodotto, ha avviato, ai sensi dell’art. 166, comma 5, del Codice, con riferimento alle specifiche situazioni di illiceità in esso richiamate, un procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2 del Regolamento, nei confronti della Società invitandola a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentita dall’Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, l. n. 689 del 24 novembre 1981).

Con il predetto atto l’Ufficio ha rilevato che la Società, in relazione alla violazione di dati personali, ha effettuato una comunicazione di dati relativi alla salute in assenza di un idoneo presupposto giuridico e, quindi, in violazione dei principi applicabili al trattamento dei dati personali, di cui agli artt. 5, par. 1 lett. a) e f) e 9 del Regolamento; con riguardo al sistema proprietario di monitoraggio del glucosio attraverso l’applicazione mobile Eversense XL la Società ha inoltre effettuato un trattamento di dati personali in violazione dei principi di liceità, correttezza e trasparenza e limitazione della finalità di cui agli artt. 5, par. 1 lett. a) e b), 6, 7, 9, 12, 13 e 15 del Regolamento e in violazione dell’art. 27 del Regolamento in quanto la nomina del rappresentante da parte di un titolare non stabilito nell’Unione è stata effettuata dalla Società solo a seguito della ricezione della richiesta di informazioni dell’Ufficio, quindi in data successiva all’avvio dei trattamenti da parte della Società stessa.

3. Memorie difensive

Con nota del XX, Senseonics ha fatto pervenire le proprie memorie difensive, senza chiedere di essere audita, fornendo altresì gli elementi di cui all’art. 83, paragrafo 2, del Regolamento, evidenziando, in particolare, quanto segue.

3.1. La violazione di dati personali ai sensi dell’art. 33 del Regolamento

La Società in relazione alla violazione di dati personali, notificata al Garante, ai sensi dell’art. 33 del Regolamento, a integrazione di quanto rappresentato nel corso dell’istruttoria preliminare, ha

dichiarato che:

"L'email in questione non [ha] fornito ai destinatari informazioni certe circa lo stato di salute degli altri destinatari per tre ragioni: 1. L'email non conteneva di per sé alcuna informazione personale relativa alla salute, ma era semplicemente una comunicazione relativa al servizio; 2. I destinatari della email non erano necessariamente pazienti, ma avrebbero potuto anche essere i loro Assistenti; 3. Gli indirizzi e-mail non contenevano necessariamente il nome dei destinatari per intero, così da permettere l'identificazione degli stessi";

"L'email era finalizzata a fornire loro informazioni relative al servizio (…). Pertanto, i destinatari delle email non erano solamente soggetti che avevano scaricato l'App Eversense nel proprio interesse (ad es. persone affette da disturbi della glicemia), ma in alcuni casi potevano anche essere degli Assistenti";

"Il contenuto dell'email era assolutamente generico ed identico per tutti i destinatari (…). La comunicazione non includeva alcun contenuto personalizzato né informazioni specifiche e personali relative ai singoli destinatari";

"Benché la grande maggioranza degli indirizzi e-mail sia da ritenersi appartenente ad utenti affetti da diabete, ragionevolmente si ritiene anche che i soggetti affetti da disturbi glicemici fossero soltanto un sottoinsieme di tutti i destinatari erroneamente inclusi nel campo CC";

"Ciò posto, l'email non conteneva di per sé informazioni personali relative alla salute dei destinatari, e, senza la raccolta di ulteriori informazioni, non era possibile per i destinatari conoscere con certezza lo stato di salute di nessuno in particolare degli altri destinatari";

"Sulla base dell'Atto di Contestazione, non vi sono ulteriori elementi per poter sostenere che tali informazioni aggiuntive idonee a rivelare lo stato di salute di un sottoinsieme dei destinatari, siano state acquisite da alcuno dei destinatari";

"Successivamente alla comunicazione ai sensi dell'Articolo 34 del GDPR, Senseonics ha ricevuto solamente qualche commento e nessuna richiesta di risarcimento danni";

"Alla luce di quanto sopra, non è possibile condividere la conclusione di codesta rispettabile Autorità che "la Società ha effettuato una comunicazione di dati relativi alla salute di 2.000 pazienti ad altrettanti pazienti";

"l'invio della mail ai destinatari in CC non è stato intenzionale ma una conseguenza di un errore umano". La violazione infatti ha riguardato un numero limitato di email inviate a clienti italiani e non ha interessato quelle inviate ad altri utenti Europei;

"l'incidente è occorso nel febbraio 2021, nel pieno corso dell'emergenza Pandemica Covid-19 (…) Il dipendente che ha inviato l'email stava lavorando da remoto. Questa circostanza potrebbe aver contribuito all'errore accidentale";

"Senseonics non ha ignorato i principi del GDPR. Al contrario, in piena conformità al principio di accountability – ai sensi dell'Articolo 5, paragrafo 2, del GDPR – (…) ha posto in essere [specifiche] azioni" quali in particolare la comunicazione della violazione agli interessati ai sensi dell'art. 34 del Regolamento e al Garante ai sensi dell'art. 33 del Regolamento;

"Alla luce di quanto sopra, (…) l'Articolo 5, paragrafo 1, lett. (a) e l'Articolo 9 del GDPR non [sono] rilevanti e non [devono] pertanto essere applicati";

"Con riguardo alla asserita violazione dell'Articolo 5, paragrafo 1, lett. (f), si ritiene che

l'Autorità avrebbe dovuto fare riferimento alle disposizioni ai sensi dell'Articolo 32 del GDPR ("Sicurezza del Trattamento") e non al generale principio di cui all'Articolo 5, lett. (f). È incontestabile che Senseonics – prima dell'invio dell'e-mail in questione – ha applicato delle misure organizzative, in conformità al principio di cui all'Articolo 5, paragrafo 1, lett. (f) (…). Un'eventuale contestazione può tutt'al più riguardare esclusivamente l'adeguatezza delle misure implementate da Senseonics, ai sensi dell'Articolo 32 del GDPR, che deve essere considerato come lex specialis" che tuttavia non è stato oggetto di contestazione".

3.2. Le ulteriori contestazioni

3.2.1 Le caratteristiche dell'App Eversense

Con specifico riferimento alle ulteriori violazioni oggetto di contestazione nell'ambito del procedimento avviato ai sensi dell'art. 166, comma 5 del Codice, la Società, dopo aver svolto alcune considerazioni di carattere preliminare con le quali ha rappresentato che Senseonics è una PMI che al termine del 2021 aveva meno di 90 dipendenti e che fornisce soluzioni innovative a pazienti che soffrono di diabete in 14 Paesi del mondo, con un numero di utenti italiani utilizzatori dell'applicazioni inferiore a 3.000-, ha dichiarato:

di aver profuso i suoi migliori sforzi per rispettare il GDPR cercando in buona fede di soddisfare tutti i requisiti previsti nel progettare un programma privacy globale;

essendo la conformità al GDPR un processo dinamico, di lavorare per cercare continuamente di migliorare nel tempo il programma di conformità nell'Unione europea;

di essere "stata significativamente colpita dalla Pandemia da Covid-19, trovandosi ad affrontare rilevanti difficoltà economiche ed organizzative, che hanno inevitabilmente rallentato la revisione dei programmi globali di compliance";

di aver "rivisto da sua informativa sulla privacy (…)", di aver "effettuato un lavoro di ingegnerizzazione finalizzato ad aggiungere al proprio prodotto schermate pop up con un testo più chiaro per la richiesta di consenso al trattamento dei dati relativi alla salute (le quali richiedono l'approvazione del BSI prima dell'implementazione)" e di aver "intrapreso ulteriori passi al fine di irrobustire il suo programma";

che l'applicazione mobile Eversense è una componente di un "sistema più complesso, il Sistema Eversense GCM, che fornisce agli utenti un monitoraggio continuo del glucosio. Tale sistema include un sensore sottocutaneo, che viene installato da un medico, e da un trasmettitore smart rimovibile, che invia i dati all'App Eversense" (…), da utilizzare congiuntamente ad un dispositivo medico impiantabile di Senseonics (…) che un cliente può utilizzare solamente sotto la supervisione di un medico";

che "In Italia i prodotti Eversense possono essere venduti solamente su prescrizione medica e possono essere acquistati solamente dagli ospedali";

che "Il download dell'App Eversense è solamente il passaggio finale a valle di un più lungo processo, con l'assistenza di un medico e – durante tale processo, che include l'impianto di un sensore sottocutaneo – l'utente è reso edotto del funzionamento del Sistema Eversense CGM e del trattamento dei dati relativi alla salute tramite l'app mobile".

3.2.2 I principi applicabili al trattamento dei dati personali

A tale riguardo, la Società ha dichiarato che:

"Il trattamento di dati personali comuni degli utenti relativi all'App Eversense non è fondato

sul consenso degli interessati. Di fatto– come già detto – il trattamento di dati personali dell'utente è necessario per la fornitura del servizio tramite l'App Eversense e pertanto la base giuridica – per tale categoria di dati personali è l'esecuzione di un contratto, ai sensi dell'Articolo 6.1, lett. (b) del GDPR";

"Con riguardo ai dati relativi alla salute, appare chiaro che il trattamento di tali dati, in linea di principio, è necessario per la funzionalità di monitoraggio del glucosio tramite l'App Eversense (…). Ciò posto dato che per il trattamento di particolari categorie di dati l'esecuzione di un contratto non può essere considerata una base giuridica valida (…) la Società ha identificato come base giuridica il consenso degli interessati, ai sensi dell'Articolo 9.2, lett. (a) del GDPR;

"La conclusione dell'Autorità che il consenso raccolto da Senseonics non è specifico non può essere condivisa. Infatti, il percorso di registrazione include una fase specifica per la raccolta del consenso privacy degli utenti";

"L'accettazione delle condizioni contrattuali e, in particolare, dell'EULA (inclusi l'Informativa sulla privacy ed i Termini d'Uso) è fornita dagli utenti cliccando sul pulsante "accetta" nella Fase 3";

"L'autorizzazione al trattamento dei dati personali, inclusi i dati relativi alla salute, è fornita dagli utenti nella Fase 4 (…), che è stata creata specificamente per fornire informazioni ed una chiara richiesta di consenso ai fini della raccolta dello stesso successivamente all'accettazione di cui alla Fase 3. La formulazione riepiloga i documenti contrattuali già accettati dall'utente, e quindi mira ad evidenziare all'utente che verrà effettuato un trattamento di dati personali";

"Il consenso raccolto nel corso della Fase 4 riguarda specificamente il trattamento dei dati personali degli utenti (e, in particolare, i dati relativi alla salute), al fine della fornitura del servizio di monitoraggio del glucosio", ciò anche in relazione a quanto rappresentato nell'informativa che menzionerebbe al riguardo i dati sensibili;

di conseguenza l'utente non sarebbe costretto a fornire il consenso in quanto "va da sé che, senza il trattamento dei livelli di glucosio dell'utente, l'App Eversense, quale componente del Sistema Eversense di Monitoraggio Continuo del Glucosio, sarebbe del tutto inutile";

L'art. 7, par. 4 del GDPR non troverebbe applicazione "in quanto pertinente soltanto laddove i dati richiesti non sono necessari per l'esecuzione del contratto (ivi compreso per la prestazione di un servizio) e l'esecuzione del contratto è subordinata all'ottenimento di tali dati in base al presupposto del consenso. Al contrario, qualora il trattamento sia necessario per eseguire il contratto (ivi incluso per la prestazione di un servizio), l'articolo 7, paragrafo 4, non si applica" (si veda par. 32, pag 11 delle Linee guida dell'EDPB sul Consenso);

"In considerazione di tali elementi, la conclusione che il consenso fornito dagli utenti sia da considerare invalido e che il conseguente trattamento di dati sia illegittimo non può essere condivisa. Al riguardo, si invita ad osservare che nell'ambito del processo in corso, volto a migliorare il livello di maturità da parte di Senseonics nell'approccio al GDPR, questa formulazione è in fase di aggiornamento".

la nuova formulazione del consenso nella quale viene esibita all'interessato la seguente formulazione "Dopo aver letto l'informativa sulla privacy, facendo clic sul tasto "Accetta", fornisco il mio consenso all'elaborazione dei miei dati sanitari affinchè Senseonics li utilizzi per offrire e gestire i Prodotti e i servizi Senseonics", verrà sottoposta all' "approvazione del BSI nel mese di febbraio 2022" e si prevede "l'approvazione e il successivo rilascio di questa

versione del software dell'app durante la primavera del 2022";

Infine, con riguardo a tutte le altre finalità del trattamento, l'Informativa Privacy chiarisce che "Nel corso della procedura di registrazione o iscrizione o in seguito ad essa, qualora ti venga richiesto di fornire un ulteriore consenso per autorizzare l'utilizzo di determinate categorie di dati, Senseonics ti contatterà direttamente per ottenere tale consenso, se si riterrà necessario ai sensi delle leggi applicabili nel tuo paese o nella tua regione in materia di protezione dei dati" (si veda il paragrafo "Iscrizione/registrazione nei Prodotti e servizi Senseonics");

In conclusione, la condotta di Senseonics non ha violato le seguenti disposizioni: Articolo 5, paragrafi 1, lett. (a), 6, 7 e 9 del GDPR.

3.2.3 L'Informativa sulla privacy per il trattamento dei dati personali

In relazione alle contestazioni aventi ad oggetto le informazioni fornite da Senseonics ai propri clienti ai sensi dell'art. 13 del Regolamento, quest'ultima ha dichiarato che:

"fornisce agli utenti informazioni esaustive sugli elementi essenziali menzionati nell'Articolo 13 del GDPR al fine di rendere gli utenti consapevoli del trattamento di dati in questione. In particolare, l'Informativa sulla privacy è totalmente chiara nello spiegare agli utenti che il trattamento relativo all'App Eversense include dati relativi alla salute";

esse "devono essere ritenute completamente allineate con le aspettative degli utilizzatori di un dispositivo medico e di una applicazione mobile le cui finalità consistono specificamente nel monitoraggio del livello di glucosio";

il "download dell'App Eversense è solo la fase finale di un lungo processo, che comincia con il confronto e la consulenza di un medico (...) Pertanto l'utilizzatore è del tutto consapevole del funzionamento del dispositivo medico e della relativa App.

"Le basi giuridiche del trattamento, anche se non specificamente menzionate in relazione a ciascuna delle finalità del trattamento, esse possono essere agevolmente dedotte dal contesto: In tutti i paesi Senseonics ha un interesse legittimo nell'offrire e utilizzare i Prodotti e servizi Senseonics perché tu ne faccia un utilizzo vantaggioso, impiegando a tal fine i tuoi dati e mettendo a tua disposizione gli aggiornamenti e le notifiche pertinenti. Inoltre (in particolare per quei paesi soggetti alle disposizioni dell'RGPD dell'Unione europea), Senseonics ti richiederà il consenso o l'autorizzazione qualora risulti necessario per un utilizzo specifico dei tuoi dati" (si veda il paragrafo "Chi controlla i tuoi dati?)";

"considerato che, come si è detto, la Società fornisce i propri prodotti in diversi Paesi a livello globale, i periodi di conservazione dei dati, al fine di rispettare gli obblighi stabiliti dalla legge, possono variare da Paese a Paese, e non era possibile menzionare nell'Informativa sulla privacy uno specifico periodo di conservazione dei dati, ma solamente i criteri applicabili, relativi alle obbligazioni contrattuali ed agli obblighi di legge; pertanto, in linea con l'Art. 13.2 del GDPR. Pertanto, l'Informativa sulla privacy menziona i criteri applicati dalla Società";

"In relazione al diritto di accesso, tali informazioni sono fornite in due distinti paragrafi dell'Informativa sulla privacy: "I tuoi diritti e le tue responsabilità" laddove è scritto "Puoi aggiornare le tue informazioni e il tuo account in qualsiasi momento effettuando l'accesso al tuo account dal nostro Sito o dall'App mobile e apportando le dovute modifiche".; "Accesso alle Informazioni" in cui viene specificato che "Qualora tu decida di esercitare il tuo diritto di richiedere la consultazione di una copia delle informazioni raccolte e conservate da Senseonics su di te, ci adopereremo in ogni modo possibile per fornirtele. Relativamente ai cittadini europei, ci atterremo alle disposizioni dell'RGPD dell'Unione europea, che ti

conferisce il diritto ad accedere alle informazioni da noi detenute su di te a seconda del trattamento in questione e nel rispetto dei limiti specifici previsti dalla stessa normativa. Qualora tu desideri richiedere l'accesso alle informazioni da noi detenute su di te in conformità alle disposizioni dell'RGPD dell'Unione europea, tale operazione potrà comportare il pagamento di 10 dollari USA (USD) a copertura dei costi ragionevoli da noi sostenuti per fornirti tali informazioni. Per presentare la suddetta richiesta, ti preghiamo di contattare dataprivacy@senseonics.com".;

"Come si è detto, il trattamento (…) è necessario per la gestione dell'account Eversense. Di conseguenza, la revoca del consenso implica la disattivazione dell'account dell'utente. Per questa ragione, gli utenti sono correttamente informati del fatto che possono disattivare il loro account (e pertanto revocare il loro consenso) e che i dati relativi al loro account saranno successivamente rimossi dai Prodotti e Servizi di Senseonics. (…) La revoca del consenso senza la disattivazione dell'account non sarebbe possibile";

"L'unica parte di informazione mancante è uno specifico riferimento al diritto degli interessati di presentare un reclamo avanti ad un'Autorità di controllo per la Protezione dei Dati. Tale riferimento verrà aggiunto nell'Informativa sulla privacy";

Con riguardo agli altri diritti degli interessati, quali la cancellazione, la limitazione e la rettifica, la Società ha rappresentato che conformemente al Regolamento essi possono essere esercitati solamente in presenza di specifiche condizioni e di ciò gli utenti sarebbero informati laddove nell'informativa viene specificato che "Tieni presente che potremmo non essere in grado di soddisfare tutte le richieste di modifica, correzione, eliminazione o limitazione e che potremmo aver bisogno di trattenere determinate informazioni per finalità di registrazione, per motivi prudenziali o legali e/o per completare tutte le transazioni avviate prima della richiesta di modifica. Nei casi in cui le Informazioni personali vengono cancellate, è possibile che alcune informazioni residue vengano ancora conservate nei nostri database e in altri registri senza essere eliminate".

La Società ha inoltre trasmesso unitamente alle memorie difensive un documento denominato "Informativa sulla privacy e condizioni di utilizzo. Data di entrata in vigore: agosto 2016; Ultimo aggiornamento settembre 2021" dichiarando che:

"successivamente alla lettera del XX del Garante, ha apportato una serie di cambiamenti nella sua Informativa sulla privacy";

tale informativa "è stata aggiornata di recente sul sito della Società (https://global.eversensediabetes.com/privacy-policy) e che essa, unitamente alla "nuova formulazione del testo della richiesta di consenso dovrebbero essere implementati nell'App Eversense con il rilascio di un aggiornamento dell'app programmato per il febbraio 2022".

3.2.4 La nomina del rappresentante stabilito nell'UE

Infine, in relazione alla nomina del rappresentante stabilito nell'UE, ai sensi dell'art. 27 del Regolamento, la Società ha rappresentato di non essere "a conoscenza del fatto che la nomina di un "authorized representative" nell'Unione europea ai sensi dell'Articolo 14 (2) della Direttiva del Consiglio 93/42/EEC [concernente i dispositivi medici] non fosse idonea a soddisfare anche i requisiti del GDPR. Solamente dopo la richiesta di informazioni da parte di codesta Autorità, Senseonics ha compreso, dopo essersi confrontata con i suoi consulenti esterni, che la nomina di tale rappresentante autorizzato non può essere sufficiente in una prospettiva GDPR e, pertanto, ha deciso di nominare specificamente un ulteriore rappresentante nell'UE, ai sensi dell'Articolo 27 del GDPR".

La Società ha pertanto chiesto all'Autorità di valutare la propria condotta come conforme al

Regolamento ovvero a “considerare tutti gli elementi del caso e, in particolare, la trasparenza di Senseonics – come dimostrata dall’immediata notificazione della violazione di dati personali occorsa nel Febbraio 2021 – ed i suoi sforzi di rispettare i principi del GDPR, considerando i miglioramenti che Senseonics ha implementato, descritti infra, e, pertanto, ad escludere l’applicazione di sanzioni pecuniarie o altre sanzioni amministrative”.

4. Esito dell’attività istruttoria

4.1 La violazione di dati personali ai sensi dell’art. 33 del Regolamento

In relazione alla violazione di dati personali, ai sensi dell’art. 33 del Regolamento, in via preliminare, si fa presente che per “dato personale” si intende “qualsiasi informazione riguardante una persona fisica identificata o identificabile (“interessato”); si considera identificabile la persona fisica che può essere identificata direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome (…)” e per “dati relativi alla salute” “i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute” (art. 4, paragrafo 1, nn. 1 e 15 del Regolamento).

Con particolare riferimento alla questione prospettata, si evidenzia che i dati personali devono essere “trattati in modo lecito corretto e trasparente” (principio di “liceità, correttezza e trasparenza”) e “in maniera da garantire un’adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di “integrità e riservatezza”)” (art. 5, par. 1, lett. a) e f) del Regolamento).
La disciplina in materia di protezione dei dati personali prevede –in ambito sanitario- che le informazioni sullo stato di salute possano essere comunicate solo all’interessato e possano essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dell’interessato stesso previa delega scritta di quest’ultimo (art. 9 Regolamento e art. 83 d.lgs. n. 196 del 30 giugno 2003 (Codice in materia di protezione dei dati personali – di seguito, il “Codice”) in combinato disposto con l’art. 22, comma 11, d.lgs. 10 agosto 2018, n. 101; cfr. anche provv. generale del 9 novembre 2005, consultabile in www.gpdt.it, doc. web n. 1191411, ritenuto compatibile con il suddetto Regolamento e con le disposizioni del decreto n. 101/2018; cfr. art. 22, comma 4, del citato d.lgs. n. 101//2018).

Tanto premesso, alla luce della definizione di dato personale sopra richiamata, gli indirizzi email sono riconducibili alla nozione di dato personale (v. Provv.ti del Garante del 25 giugno 2002, doc. web n. 29864 e del 24 giugno 2003, doc. web n. 1132562). Pertanto, anche se una parte degli indirizzi email erano privi di riferimenti al nome dei destinatari per intero o comunque ad altri dati direttamente identificativi degli interessati, si tratta di informazioni di natura personale, soggette, come le altre, all’applicazione della disciplina in materia di protezione dei dati personali.

Inoltre, con riguardo al caso di specie, le informazioni oggetto della notifica, contenute nella richiamata email, seppure riferita ad una comunicazione di servizio, essendo indirizzata a soggetti utilizzatori del sistema di monitoraggio del glucosio Eversense XL, costituiscono dati personali relativi alla salute. Infatti, tale sistema è destinato alle persone che desiderano gestire attivamente il proprio diabete con semplicità e sicurezza, tramite un sensore impiantabile, uno Smart Transmitter rimovibile e ricaricabile e una applicazione per smartphone (cfr. provv. 25 giugno 2002, doc. web n. 29864; provv. del 9 gennaio 2020, doc. web 9261234; provv. del 13 maggio 2021, doc. web n. 9688020). La circostanza che tra i destinatari possano essere presenti non solo i pazienti ma anche i loro assistenti (caretaker) non determina una diversa qualificazione di tali informazioni come appartenenti alle categorie particolari di dati atteso che il contenuto della email faceva inequivocabilmente riferimento alla presenza di una patologia diabetica e che gli indirizzi dei destinatari erano quelli che i pazienti avevano fornito proprio in relazione alla predetta

patologia. Si evidenzia inoltre che la stessa Azienda nella notifica di violazione ha qualificato tali informazioni come relative alla salute.

In relazione al principio di integrità e riservatezza di cui all'art. 5, par. 1, lett. f) del Regolamento, esso prevede che i dati personali siano trattati "in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali". La circostanza che nell'atto di contestazione, l'Ufficio oltre all'effettuato richiamo all'art. 5, par. 1 lett. f) del Regolamento avrebbe dovuto fare riferimento anche alla violazione dell'art. 32 del Regolamento ciò in quanto la Società – prima dell'invio dell'email in questione – avrebbe applicato misure organizzative, in conformità al predetto principio e pertanto la contestazione avrebbe dovuto avere ad oggetto esclusivamente l'adeguatezza delle misure implementate, non può essere accolta.

Infatti, il predetto art. 5, par. 1, lett. f) del Regolamento impone ai titolari di trattare i dati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate. Esso pertanto introduce un principio da cui scaturisce l'obbligo di trattare i dati in modo da garantirne l'integrità e la riservatezza, la cui violazione è sanzionabile ai sensi dell'art. 83, par. 5 del Regolamento. È evidente che nel caso di specie le misure tecniche ed organizzative implementate non fossero adeguate atteso che si è realizzata la violazione di dati personali oggetto di notificazione da parte del titolare del trattamento (cfr. par. 6.2 delle Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021; provv.to del 13 maggio 2021, doc. web 9688020; provv. del 16 settembre 2021, doc. web 9722297 e provv.to del 28 aprile 2022 n. 164, in corso di pubblicazione). Del resto la stessa Società, nel corso dell'istruttoria ha previsto l'adozione di ulteriori misure organizzative proprio al fine evitare il ripetersi di eventi analoghi a quello occorso

Pertanto, l'invio di comunicazioni mediante un unico messaggio di posta elettronica indirizzato a un numero plurimo di destinatari, i cui indirizzi sono stati inseriti nel campo copia conoscenza (c.c.), ha, di fatto, senza giustificato motivo e in assenza di idoneo presupposto giuridico, rivelato reciprocamente, ai destinatari delle comunicazioni, lo stato di salute degli altri pazienti comportando un trattamento di dati sulla salute in violazione degli artt. 5, par. 1 lett. a) e f) e 9 del Regolamento.

4.2. Le ulteriori violazioni

4.2.1 I Principi di liceità e limitazione della finalità del trattamento dei dati personali (art. 5, par. 1, lett. a) e b) del Regolamento)

In prima battuta l'Ufficio, in relazione ai trattamenti effettuati dalla Società attraverso il sistema di monitoraggio del glucosio Eversense XL e l'applicazione mobile, ha contestato la violazione dell'art. 5, par. 1, lett. a) e b) del Regolamento, il quale prevede il rispetto del principio di liceità, in base al quale ogni trattamento di dati personali deve fondarsi su uno specifico presupposto giuridico, e di limitazione della finalità, per cui i dati possono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità.

Nel caso in cui la condizione di liceità sia rappresentata dal consenso, esso deve essere prestato attraverso un atto positivo con il quale l'interessato manifesta una volontà libera, specifica, informata e inequivocabile relativa al trattamento dei dati personali che lo riguardano. Qualora il trattamento è volto a perseguire una pluralità di finalità -come nella fattispecie in esame- il consenso deve essere prestato per ciascuna di tali finalità (Considerando 32, 42 e 43, artt. 5, 6, par. 1, lett. a) e 7 del Regolamento e Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679, adottate dal Comitato europeo per la protezione dei dati personali, il 4 maggio 2020; sent. C-673/17, del 1° ottobre 2019 e C-61/19, dell'11 novembre 2020).

Con specifico riferimento alle particolari categorie di dati, tra cui rientrano i dati sulla salute, l'art. 9 del Regolamento sancisce un generale divieto al trattamento di tali dati a meno che non ricorra una delle specifiche esenzioni a tale divieto tra le quali è previsto il consenso dell'interessato. Tale consenso, tenuto conto della natura di tali dati, particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, deve essere anche esplicito (art. 9, par. 2 lett. a) del Regolamento e par. 4 delle Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679, adottate dal Comitato europeo per la protezione dei dati personali il 4 maggio 2020).

Nel caso di specie, dalla documentazione in atti risulta accertata la violazione del principio di liceità del trattamento, in quanto all'epoca dei fatti, in occasione del download della applicazione (cfr. l'allegato 2 alla nota della Società, del XX), con un unico "clic" sul tasto "accetto" gli utenti erano chiamati ad accettare sia "i termini del contratto di licenza con l'utente finale" che "l'informativa privacy e le condizioni di utilizzo di Senseonics, autorizzando contestualmente la conservazione, la trasmissione e l'uso dei dati, comprese, senza limitazioni la conservazione nel Regno Unito, la trasmissione negli USA per finalità limitate (ad esempio ingegneristiche e di assistenza clienti) secondo i termini dell'EULA e dell'informativa privacy".

Pertanto, la circostanza che sia stato richiesto un unico atto dispositivo da parte dell'interessato determina il mancato rispetto del requisito della specificità del consenso per le diverse finalità perseguite dal titolare del trattamento, ciò a maggior ragione in relazione al trattamento dei dati sulla salute, rispetto ai quali, il consenso deve altresì essere esplicito (art. 9, par. 2, lett. a) del Regolamento). Sul punto, le richiamate Linee Guida 5/2020 sul consenso, chiariscono due aspetti rilevanti in relazione alla fattispecie in esame. Da una parte, che "con "azione positiva inequivocabile" si intende che l'interessato deve aver intrapreso un'azione deliberata per acconsentire al trattamento specifico" dall'altra che "Il titolare del trattamento deve (…) fare attenzione al fatto che il consenso non può essere ottenuto tramite la stessa azione con cui si accetta un contratto o le condizioni generali di servizio. L'accettazione globale delle condizioni generali di contratto/servizio non può essere considerata come un'azione positiva inequivocabile ai fini del consenso all'uso dei dati personali" (cfr. punti 77 e 83). Inoltre, tenuto conto che con riguardo al trattamento dei dati sulla salute, la base giuridica del trattamento non può che rinvenirsi in una delle deroghe al generale divieto di trattare tale categoria di dati, elencate all'art. 9, par. 2 del Regolamento, si ritiene inconferente il richiamo all'art. 7, par. 4 del Regolamento e al punto 32 delle richiamate Linee Guida sul consenso che fanno riferimento invece ai trattamenti di dati diversi da quelli sulla salute svolti per l'esecuzione di un contratto compresa la prestazione di un servizio (art. 6, par. 2, lett. b) del Regolamento).

Con specifico riferimento alle finalità del trattamento, esse non risultano chiaramente determinate, né esplicitate agli interessati (v. infra). Le finalità del trattamento dei dati personali, infatti, nel rispetto del principio di trasparenza, devono essere esplicite e legittime e precisate al momento della raccolta dei dati personali. Nel caso, in esame, le stesse sono state chiaramente rappresentate dalla Società solo nella nota di riscontro alla richiamata richiesta di informazioni.

4.2.2 Il principio di trasparenza e le informazioni da rendere agli interessati (artt. 5, par. 1, lett. a), 12 e 13 del Regolamento)

I dati personali devono essere trattati nel rispetto del principio di trasparenza (art. 5, par. 1 lett. a) del Regolamenti) fornendo preventivamente agli interessati le informazioni di cui all'art. 13 del Regolamento, in caso di dati raccolti direttamente presso di essi, ovvero ai sensi dell'art. 14, in caso di dati raccolti presso soggetti terzi. Tale principio impone che le informazioni e le comunicazioni relative al trattamento dei dati personali siano rese in una forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (cons. 39, 58 e art. 12 del Regolamento).

L'obbligo di fornire agli interessati le informazioni in forma "concisa e trasparente" implica che il

titolare del trattamento presenti le informazioni in maniera efficace e succinta al fine di evitare un “subissamento” informativo. Esse dovrebbero essere “nettamente differenziate dalle altre informazioni che non riguardano la vita privata, quali clausole contrattuali o condizioni generali d’uso” e dovrebbero essere “concrete e certe, non dovrebbero essere formulate in termini astratti o ambigui né lasciare spazio a interpretazioni multiple” (cfr. punti 8 e 12, delle Linee guida sulla trasparenza ai sensi del regolamento 2016/679, adottate dal Gruppo Articolo 29, il 29 novembre 2017, versione emendata adottata l’11 aprile 2018 e paragrafo e paragrafo 3.7).

Nel contesto delle applicazioni che sono in grado di raccogliere grandi quantità di dati dal dispositivo (ad esempio dati memorizzati dall'utente e dati da diversi sensori, tra cui la geolocalizzazione), l'utente finale ha il diritto di sapere che tipo di dati personali sono oggetto di trattamento, per quali finalità si intendono utilizzare e sulla base di quali presupposti giuridici. La disponibilità di queste informazioni è infatti fondamentale per ottenere il consenso al trattamento dei dati personali dell’utente, che può ritenersi valido solo se l'interessato è stato previamente informato in merito agli elementi chiave del trattamento dei dati e quindi consapevole delle scelte in materia di trattamento dati che sta effettuando attraverso la manifestazione del consenso. Inoltre, si dovrebbe comunicare agli utenti con un linguaggio semplice e chiaro se i dati potranno essere riutilizzati da terzi e in tal caso per quali scopi. Indicazioni generiche come "innovazione del prodotto" sono inadeguate per informare gli utenti (cfr. paragrafo 3.7 del Parere 02/2013, sulle applicazioni per dispositivi intelligenti adottato il 27 febbraio 2013).

In ossequio al principio di trasparenza devono quindi risultare chiare, prima che il trattamento abbia inizio, sia se finalità che le corrispondenti basi giuridiche del trattamento.

Al riguardo, si evidenzia che il modello di informativa acquisito in atti, in riscontro alla richiesta di informazioni della Società, del XX, realizzato da quest’ultima in qualità di titolare del trattamento, è risultato non conforme al richiamato quadro normativo in materia di protezione dei dati personali, in quanto privo di alcuni degli elementi essenziali previsti dalla disciplina vigente:

- il documento denominato “informativa sulla privacy e condizioni di utilizzo” (PPTOU”, Privacy policy & Terms of Use)” reca al proprio interno molteplici sezioni che non riguardano il trattamento dei dati personali (ad es. “Politica di Senseonics nei confronti dei minori”; “Diritti di autore, marchi e utilizzo”; “Esclusione di garanzie limitazioni di Responsabilità”;

- non risultano chiaramente individuate le finalità del trattamento in una forma concisa, intellegibile e facilmente accessibile. Esse infatti dovrebbero essere desunte dagli interessati accedendo a diverse sezioni dell’informativa, tra l’altro non sempre pertinenti quali quelle denominate “Modalità di utilizzo dei dati”; “App Mobili e siti”; “Richieste di Senseonics”;

- non risultano indicate le basi giuridiche del trattamento, che non possono essere dedotte dal contesto, in quanto -come sopra evidenziato- esse rappresentano un’informazione essenziale tra quelle da rendere agli interessati e devono pertanto essere chiaramente individuate rispetto alle diverse finalità perseguite dal titolare del trattamento;

- non risultano indicati i tempi di conservazione dei dati e neppure possono ritenersi definiti i relativi criteri di conservazione dei dati, laddove si fa ad esempio riferimento alla necessità di trattenere determinate informazioni “per motivi prudenziali”. A tale riguardo, le richiamate Linee Guida sulla trasparenza hanno chiarito come l’individuazione dei tempi di conservazione deve essere strettamente collegato all’obbligo di minimizzazione dei dati e di limitazione della conservazione (art. 5, paragrafo 1, lettera c) e) del Regolamento). Pertanto, non può ritenersi sufficiente che “il titolare del trattamento affermi in maniera generica che i dati personali saranno conservati finché sarà necessario per le finalità legittime del trattamento. Ove pertinente, dovrebbero essere fissati periodi di conservazione diversi per le diverse categorie di dati personali e/o finalità del trattamento, inclusi, se del caso, i periodi di

archiviazione" (cfr. Allegato "Informazioni da fornire all'interessato ai sensi dell'articolo 13 o 14" delle Linee Guida sulla trasparenza, WP260, rev. 1);

non risulta indicata la facoltà di revoca del consenso per i trattamenti basati su tale condizione di liceità, quali i trattamenti dei dati sulla salute ai sensi dell'art. 9, par. 2, lett. a) del Regolamento, né essa può ritenersi implicita nell'operazione di disattivazione dell'account Senseonics. L'utente infatti potrebbe disattivare il proprio account per ragioni non connesse ai profili di protezione dei dati. In ogni caso in base all'art. 7, par. 3 del Regolamento, il titolare del trattamento deve informare l'interessato del diritto di revoca prima che quest'ultimo presti effettivamente il consenso;

non risultano chiaramente indicati nell'informativa generale i diritti spettanti agli interessati ai sensi degli articoli da 15 a 22 del Regolamento, e in particolare il diritto di accesso ai dati;

da ultimo, non risulta indicato il diritto di proporre reclamo all'Autorità di controllo.

4.2.3 L'esercizio dei diritti degli interessati (art. 12, 13 e 15 del Regolamento)

Il Regolamento fissa le regole generali che si applicano alla fornitura d'informazioni agli interessati (ai sensi degli articoli 13 e 14) e alla comunicazione con gli interessati riguardo all'esercizio dei loro diritti, ai sensi degli articoli 15-22 (art. 12 del Regolamento). In particolare, l'obbligo di trasparenza relativo al trattamento dei dati personali è un obbligo trasversale che si esplica in tre elementi centrali tra cui rilevano anche le modalità con le quali il titolare del trattamento agevola agli interessati l'esercizio dei diritti di cui godono. Contestualmente alla raccolta di dati personali, il titolare del trattamento è infatti tenuto a fornire all'interessato, al fine di garantire un trattamento corretto e trasparente, le informazioni anche in ordine, all'esistenza dei diritti ad esso riconosciuti dagli artt. da 15 a 22 del Regolamento (art. 13, par. 2, lett. b) del Regolamento).

Al riguardo, si evidenzia che il documento denominato "Informativa sulla privacy e condizioni di utilizzo" nella sezione i tuoi diritti e le tue responsabilità non reca alcun riferimento al diritto di accesso degli interessati, ciò in violazione dell'art. 13, par. 2 lett. b) del Regolamento. La sezione "accesso alle informazioni" riguarda infatti l'informativa sui cookies.

Pertanto, il comportamento della Società che ha omesso di citare il diritto di accesso ai dati previsto dall'art. 15 del Regolamento si pone in contrasto non solo con quanto previsto dagli artt. 13 e 15 del Regolamento ma anche in violazione dell'art. 12, laddove sono fornite indicazioni puntuali in ordine alle modalità con le quali titolare ed interessato dovrebbero rapportarsi con riferimento, tra l'altro, all'esercizio dei diritti da parte di quest'ultimo.

4.2.4 La nomina di un rappresentante stabilito nell'UE

L'art. 27 del Regolamento prevede che, ove si applichi l'art. 3, par. 2, il titolare è tenuto a designare per iscritto un rappresentante nell'Unione europea, il quale deve essere stabilito in uno degli Stati membri in cui si trovano gli interessati i cui dati sono trattati nell'ambito dell'offerta di beni e servizi o il cui comportamento è monitorato e che funge da interlocutore, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.

Nel caso di specie, non v'è dubbio che siano integrati i presupposti di applicabilità dell'art. 3, par. 2, lett. a) del Regolamento; Senseonics, infatti, tratta dati personali di interessati che si trovano nell'Unione e le sue attività di trattamento sono connesse alla prestazione di servizi ad utenti europei.

La Società era tenuta quindi a designare, mediante mandato scritto, un rappresentante nel territorio unionale incaricandolo ad interagire per suo conto con riguardo agli obblighi che derivano dal Regolamento anche per quanto riguarda la cooperazione con l'Autorità di controllo. La

mancata nomina di tale rappresentante fino al 29 giugno 2021, data successiva all'avvio dell'istruttoria preliminare da parte del Garante, integra pertanto la violazione dell'art. 27 del Regolamento.

4.2.5 Le ulteriori criticità relative all'informativa trasmessa

In relazione al documento in atti, trasmesso dalla Società unitamente agli scritti difensivi, persistono specifici profili di non conformità rispetto al richiamato quadro normativo in materia di protezione dei dati personali, in quanto:

- il documento continua ad essere erroneamente denominato "Informativa privacy e condizioni di utilizzo", recando al proprio interno molteplici sezioni che non riguardano il trattamento dei dati personali (ad es. "Politica di Senseonics nei confronti dei minori"; "Diritti di autore, marchi e utilizzo"; "Esclusione di garanzie limitazioni di Responsabilità";

- non risultano chiaramente individuate le finalità del trattamento in una forma concisa, intellegibile e facilmente accessibile. Esse infatti dovrebbero essere desunte dagli interessati accedendo a diverse sezioni dell'informativa, tra l'altro non pertinenti quali quelle denominate "Modalità di utilizzo dei dati"; "App Mobili e siti"; "Richieste di Senseonics";

- non è chiaro se la sezione "scopo" della nuova tabella inserita nel documento recante le basi giuridiche del trattamento applicabili agli utenti dell'Unione europea prevale rispetto alle molteplici finalità desumibili dall'intero documento;

- in relazione alle finalità di marketing, per le quali è previsto l'utilizzo non solo delle email ma anche di altri mezzi di comunicazione (il documento fa generico riferimento a "note"/"avvisi"), è necessario che tale trattamento si fondi su una specifica base giuridica. A tale riguardo rileva altresì l'art. 130 del Codice il quale richiede di acquisire uno specifico consenso da parte degli interessati qualora sia previsto l'uso di sistemi di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o di comunicazione commerciale;

- nella sezione denominata "quali categorie di dati viene raccolta da Senseonics" è riportata la seguente frase "Utilizzando i Prodotti e servizi Senseonics, accetti che noi raccogliamo, trasferiamo, conserviamo e/o trattiamo le tue informazioni per le finalità descritte nel presente documento PPTOU", di fatto prevedendo un generico consenso implicito al trattamento dei dati per tutte le finalità ivi indicate, in palese contrasto non solo con la normativa in materia di protezione dei dati personali (cfr. par. 3.2.1), ma anche con l'elencazione delle basi giuridiche del trattamento, di cui alla successiva tabella indicata nel documento;

- nell'informativa generale non sono indicati i diritti spettanti agli interessati ai sensi degli articoli da 15 a 22 del Regolamento.

5. Conclusioni

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare nel corso dell'istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice gli elementi forniti dal titolare del trattamento nella memoria difensiva, seppure meritevoli di considerazione, non consentono di superare gran parte dei rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni si rileva l'illiceità del trattamento di dati personali effettuato dalla Società in violazione degli articoli 5, par. 1 lett. a), b) e f), 6, 7, 9, 12, 13, e 27 del Regolamento. La violazione

delle predette disposizioni rende, altresì, applicabile la sanzione amministrativa prevista dall'art. 83, par. 4 e 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo.

6. Misure correttive

L'art. 58, par. 2, prevede in capo al Garante una serie di poteri correttivi, di natura prescrittiva e sanzionatoria, da esercitare nel caso in cui venga accertato un trattamento illecito di dati personali.

Tra questi poteri, l'art. 58, par. 2, lett. d) del Regolamento, prevede il potere di "ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine".

Alla luce delle valutazioni sopra richiamate, si ritiene di dover ingiungere alla Società, ai sensi del richiamato art. 58, par. 2, lett. d) Regolamento, di adottare entro novanta giorni dalla notifica del presente provvedimento, le seguenti misure correttive:

1. di rielaborare il documento denominato "Informativa sulla privacy e condizioni di utilizzo" in una forma concisa, trasparente e intellegibile, eliminando altresì le sezioni non pertinenti rispetto ai profili di protezione dei dati personali quali ad es. la "Politica di Senseonics nei confronti dei minori"; "Diritti di autore, marchi e utilizzo"; "Esclusione di garanzie limitazioni di Responsabilità" e il riferimento alle "condizioni di utilizzo";

2. di indicare chiaramente nel richiamato documento la specifica sezione relativa ai trattamenti di dati personali effettuati nei confronti di interessati dell'Unione europea, nella quale è necessario fare espresso riferimento al quadro normativo in materia di protezione dei dati personali ad essi applicabile e in particolare all'art. 13 del Regolamento.

3. di indicare nel medesimo documento, in una forma concisa, trasparente e intellegibile tutte le informazioni previste dall'art. 13 del Regolamento;

4. di individuare, rispetto a ciascuna delle finalità perseguite, idonee basi giuridiche, tenendo in debita considerazione quelle previste dall'art. 9, par. 2 del Regolamento per il trattamento dei dati sulla salute;

5. di individuare nell'informativa generale i diritti spettanti agli interessati ai sensi degli articoli da 15 a 22 del Regolamento;

6. di confermare che l'informativa sulla privacy sia stata integrata prevedendo il diritto degli interessati di presentare un reclamo avanti all'Autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, qualora ritenga che il trattamento che lo riguardi violi il Regolamento (art. 77, par. 1 del Regolamento).

7. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

La violazione degli artt. 5, par. 1 lett. a), b) e f), 6, 7, 9, 12, 13, e 27 del Regolamento, causata dalla condotta posta in essere da Senseonics Inc. è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4, lett. a) e 5, lett. a) e b) del Regolamento.

Il Garante, ai sensi ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo

83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenuto conto dei principi di effettività, proporzionalità e dissuasività, indicati nell'art. 83, par. 1, del Regolamento, alla luce degli elementi previsti all'art. 83, par. 2 e, del Regolamento. In relazione alla violazione di dati personali notificata dal titolare del trattamento, ai sensi dell'art. 33 del Regolamento, si osserva che:

1. il trattamento effettuato ha riguardato informazioni idonee a rilevare lo stato di salute di circa 2000 interessati, seppure non di tutti in quanto "gli indirizzi email dei destinatari non contenevano necessariamente il nome per intero" (art. 4, par. 1, n. 15 del Regolamento e art. 83, par. 2, lett. a) e g) del Regolamento);

2. l'Autorità è venuta a conoscenza della violazione, tramite la notifica della violazione, effettuata dalla Società il XX e non sono pervenuti segnalazioni o reclami rispetto a tale condotta (art. 83, par. 2, lett. h) del Regolamento);

3. sotto il profilo riguardante l'elemento soggettivo non emerge alcun atteggiamento intenzionale da parte del titolare del trattamento essendo la violazione avvenuta in conseguenza di un errore umano nell'invio dell'email (seppure caratterizzato da colpa grave tenuto conto che il dipendente aveva ricevuto specifiche istruzioni circa la necessità di nascondere l'indirizzo di tutti i pazienti in occasione dell'invio di comunicazioni tramite email), (art. 83, par. 2, lett. b) del Regolamento);

4. non risultano, precedenti violazioni pertinenti commesse dal titolare del trattamento, né sono stati precedentemente disposti provvedimenti di cui all'art. 58 del Regolamento (art. 83, par. 2, lett. e) del Regolamento);

5. la Società ha collaborato pienamente con l'Autorità nel corso dell'istruttoria e del presente procedimento (art. 83, par. 2, lett. f) del Regolamento);

6. il titolare del trattamento, non appena venuto a conoscenza della violazione ha adottato delle misure organizzative volte a evitare la ripetizione della condotta illecita, prevedendo:

   una analisi "di tutte le altre e-mail inviate per assicurarsi che l'errore non fosse stato ripetuto in altri gruppi di email";

   (…) "un processo di conferma al fine di monitorare, rivedere ed assicurare che l'email di chiarimenti fosse adeguatamente rivolta ed inviata ai destinatari corretti, e che l'errore non venisse ripetuto";

   per le future e occasionali comunicazioni dirette agli utenti, di richiedere "come accorgimento ulteriore (…) (come abbiamo fatto con l'email correttiva) una mail di conferma che la pratica di includere gli indirizzi nel campo ccn sia eseguita correttamente" (art. 83, par. 2, lett.c) del Regolamento).

In relazione alle restanti violazioni si osserva che:

7. non risultano, precedenti violazioni pertinenti commesse dal titolare del trattamento né sono stati precedentemente disposti provvedimenti di cui all'art. 58 del Regolamento (art. 83,

par. 2, lett. e) del Regolamento);

8. la Società ha collaborato pienamente con l'Autorità nel corso dell'istruttoria e del presente procedimento (art. 83, par. 2, lett. f) del Regolamento);

9. la Società ha posto in essere alcune misure volte a conformare il trattamento dei dati personali al quadro normativo vigente in materia di protezione dei dati personali, tuttavia persistono i profili di non conformità sopra evidenziati (par. 6)

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, par. 5, lett. a) del Regolamento, nella misura di € 45.000,00 (quarantacinquemila) per la violazione degli artt. 5, par. 1 lett. a), b) e f), 6, 7, 9, 12, 13 e 27 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1 e 3, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019, anche in considerazione della tipologia di dati personali oggetto di illecito trattamento.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato da Senseonics Inc, con sede legale in 20451 Seneca Meadows Parkway - Germantown, MD 20876-7005, USA, in persona del legale rappresentante pro-tempore rappresentata e difesa dall'XX, giusta procura speciale in atti, per la violazione degli dell'artt. 5, par. 1 lett. a), b) e f), 6, 7, 9, 12, 13 e 27 del Regolamento nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, a Senseonics Inc, di pagare la somma di € 45.000,00 (quarantacinquemila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata.

INGIUNGE

A Senseonics Inc.:

di pagare la somma di euro € 45.000,00 (quarantacinquemila) -in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice-, secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981;

ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di conformare i trattamenti alle disposizioni del Regolamento, adottando le misure correttive indicate nel paragrafo 6 del presente provvedimento, entro e non oltre il termine di 90 giorni dalla notifica del presente provvedimento. L'inosservanza di un ordine formulato ai sensi dell'art. 58,

par. 2, del Regolamento, è punita con la sanzione amministrativa di cui all'art. 83, par. 6, del Regolamento;

ai sensi dell'art. 58, par. 1, lett. a), del Regolamento e dell'art. 157 del Codice, di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto prescritto nel predetto par. 6, e di fornire comunque riscontro, adeguatamente documentato, entro e non oltre il termine di 20 giorni dalla scadenza del termine sopra indicato. Il mancato riscontro a una richiesta formulata ai sensi dell'art. 157 del Codice è punito con la sanzione amministrativa, ai sensi del combinato disposto di cui agli artt. 83, par. 5, del Regolamento e 166 del Codice.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 7 luglio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei